Title
Social choice and technical problems in electronic funds transfer systems

Permalink
https://escholarship.org/uc/item/57s320cb

Author
Kling, Rob

Publication Date
1977

Peer reviewed
Social Choice and Technical Problems in Electronic Funds Transfer Systems

Rob Kling

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

Technical Report #102

Department of Information and Computer Science, University of California Irvine, CA 92717.
Abstract

Over the last decade, plans for using computer-based systems 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 systems for Electronic Funds Transfer (EFT) are not to cause more problems for the larger public than they solve. This paper examines the benefits that EFTs may provide and the social problems they raise in the context of enduring value conflicts.

CR. Categories: 2.11, 2.12, 2.3, 3.32, 3.33, 3.55

Key Words: Electronics Fund Transfer Systems, Social Impacts, Privacy, Social Choice, Networks, Network Reliability, Security, Values
**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.[8,11].

The various Electronic Funds Transfer (EFT) systems that 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

* Electronic funds transfer systems comprise those technologies that are used to transmit credits, debits, or related business information computing and/or communications technologies. The term is often used loosely to describe a wide variety of computer-related technologies that are being used by banks and businesses to process and store financial transactions and related information.
networks, 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. 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. Fedwire and Bankwire transmit tens of billions of dollars in large interbank transactions each day[34]. But at this time, however, there are no networks which automate the processing of checks between personal accounts at different banks.

Several dozen major financial institutions, government agencies, and computer vendors are developing EFT technologies and their associated administrative frameworks. It is a fast-moving "social world" in which events outpace rumors of events[20]. 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. An extremely fragmented literature describing different aspects of EFTs has grown at an enormous pace during the last few years. A few special studies include a broad range of problems that are that EFTs may foster. However, the widely published articles and most of the special reports address the interests of financial, business, and technical groups that would directly benefit from different EFT arrangements. This is due, in part, to the sheer complexity and
variety of issues that EFTs raise. Few specialists can write authoritatively and insightfully about the technical, economic, regulatory, legal, political, and social aspects of EFTs. Even then, the resulting analyses would often be too complex and lengthy for most journals. 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 EFT development. These commitments help create a literature in which analysis and advocacy are subtly intertwined.

Most analysts view EFTs as "economic instruments" whose costs and benefits may be assessed adequately in dollars**. This paper views EFTs as both an economic and "political instrument." As a political instrument, it may induce important shifts of social power, which because they are relatively intangible, are difficult to analyze.

The analytic framework developed in this paper centers upon idealized value positions. These provide criteria for social choices which include, but are not limited to, economic considerations. Some social activities that may be catalyzed by EFTs, such as regulatory impediments to EFT developments, consumer indifference to EFT-related services, "credit blackouts," large scale theft or political surveillance, are substantially more troublesome for parties that hold one value position than for parties that hold another. As we shall

** See [9] for an exception.
see, EFIs developments can 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 lifestyles and our political system.

This article analyzes several major unresolved social and technical problems that may develop as side effects of EFIs and places them in a context in which their relation to important common, but often conflicting, value positions is apparent. Prior to that analysis, the principles of a simplified EFT technology are described and the major value positions are elaborated.

Sample EFIs:

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 EFIs, their features will be elaborated here. Unfortunately, a definitive description of automated check processing

This article treats only a few major issues catalyzed by EFT developments. Many issues, such as the impacts of EFIs on the U.S. Postal Service are outside the scope of this article. See [Agenda] for a list of bi emerging research issues. See [3, 34] for descriptions of several additional EFIs.
operations is impeded by the absence of detailed, comprehensive proposals in the literature \cite{13,6,8,11,12,13,25,35}. And, it is possible that EFTs which are initially designed and implemented separately will be coupled at a later time\cite{25}. 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.)

10. The New York City Federal 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 (8,10) 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 individual 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 [26]. 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.
On the other hand, several different Federal Reserve regions are experimenting with "automated clearing houses." These arrangements allow pre-authorized debits to be extracted from payroll checks and pre-authorized credits (such as social security checks) to be deposited into individual accounts. The current experiments operate in batch mode with transaction tapes from several sources being processed at special regional centers. These ACHs are providing the current experimental basis for ACPS. Nevertheless, it may turn out that the largest volume of electronic transactions during the next decade will be processed via a sales-related networks rather than through ACPS.

Value Positions for Assessing EFTs

EFTs are a technical instrument; a means to some end. Proposals for "preferred" EFT arrangements often assume some particular social goods should be maximized. At least six major value orientations seem to be implicit in the published discussions of EFTs. In different instances, they may be mutually 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, EFT developments which are congruent with any of these positions might be argued to be in "the public interest."
1. **A Free Enterprise Model**: The preeminent consideration is profitability of the EFIs 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.

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.

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 EFIs 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.

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

---

* 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?" [21].
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. On the other hand, government regulations requiring financial institutions using EFls to keep detailed archival records of the transactions processed may be most congruent with a Statist position. It would compromise both Libertarian and Free Enterprise positions. This would especially be the case if the records were kept at the expense of the EFl using business and occasionally searched by government agencies wishing to audit the activities of selected persons or groups.

Some publics may be best served by EFl developments most consistent with the value positions listed above. Some of these publics, such as large businesses and government agencies are relatively well organized to influence EFl arrangements. Generally, publics with Free Enterprise or Statist interests are best organized. In contrast, the publics best served by the Populist and Libertarian positions are poorly organized.

In addition, publics whose interests are aligned with a common value position, may also be in conflict with each other. For example, while business interests are most closely aligned with the Free Enterprise position, particular businesses may be in sheer competition with each other for specific markets. In this article, the benefits and problems catalyzed by EFls are analyzed in relation to the value positions developed here rather than in relation to the sheer clash of conflicting groups.
In general, EFTs have been most forcefully advocated and developed by groups that advocate predominantly Free Enterprise and Statist criteria for social choice. 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 EFT 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 EFT developments, it is unlikely that they will be "solved." Rather, different EFTs arrangements 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.

**EFT Benefits and Social Values**

EFTs are advocated by the Federal Reserve Board, major banking institutions, charge card companies, and others as providing a variety of economic benefits for its users and consumers. These include:

1. Cutting the cost of check processing*;

* Checks alone were estimated to cost $5 billion to process in 1973 [10].
2. Diminishing the losses from petty theft;
3. Providing mechanisms for allowing pre-authorized payments;
4. Real time credit verification;
5. Decreased float;
6. Convenient adjunct services;
7. Providing timely and comprehensive market information;
8. Increasing the potential market share of commercial users.

These benefits are well described elsewhere[7,8,11,15,18,24,25]. Here we wish to make a few simple observations. First, some of these benefits are more important than others to EFT promoters. For example, some studies show that it is unlikely that banks would make major savings in the costs of paper handling with ACPS[3]. Rather, fear and hope drives many financial institutions into developing EFTs. An institution that develops EFT related services may gain new customers; an institution that delays much longer than its competitors may lose out[25].

Secondly, some of the benefits which accrue to an EFT user may be offset by other major changes in the economy or financial system. For example, ACPS may decrease float and EFTs regulated by the Federal Reserve Board (Fed) could lead banks to reenter the Federal Reserve System. Both of these independent events could help enhance the control that the Fed exerts over monetary policy[5]. However, such increased control could be offset by EFT arrangements which promote increased credit or by new congressional controls over the Fed.
This example illustrates the conflicting impacts of different EFT components. ACPS may be in part deflationary while PUS nets may be inflationary in their gross economic impact. These examples also illustrate the ways in which EFT benefits may accrue more to one party than to others. For example, many individual consumers and businesses cherish float more than the Fed; some businesses may prosper with EFT support while others may whither. Lastly, most of these issues are cast in the context of Free Enterprise and Statist values. At best, they do not compromise activities based on other value positions, such as the Populist and Libertarian positions.

**EFT Problems and Social Values**

Some accounts identify emerging EFTs with social progress. 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 EFT developments." [25, p. 2]
Unfortunately, such a sanguine view simply glosses the sheer possibility of social problems and fundamental value conflicts fostered by a new technology such as EFT. 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.

This section is devoted to explaining some of the potential troubles that most compromise the Populist and Libertarian positions. As we shall see, some of the issues which are troublesome for these positions are also troublesome for interests consistent with the other positions as well.

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 newsmen 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 across 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.

EFT 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 Minookee, one must be in Minookee. 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 legitimately 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.

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(25). 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*.

* 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 a rather general protection scheme[14].
3. The body of techniques for developing technically secure systems is growing rapidly [17, 25, 29, 32, 36]. 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 [23].

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. 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.

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 EFIs is even more primitive. In short, an electronic Fort Knox is still a technical dream, not a contemporary reality.

   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

---

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[1,28].

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 transferred real-time in a network linking PUS
terminals and ACPS is provided in [18].

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[23]. 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 viability 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 thieves may attempt to extort as well as bribe or co-opt employees of financial institutions who know certain sensitive details of EFl 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, maintenance staff, bank auditors, etc.) would number in the tens of thousands. These problems of maintaining the integrity of people who have sensitive knowledge of EFls operations may turn out to far exceed the technical problems of system security both in magnitude and difficulty.

In theory large scale theft doesn't serve any legitimate interest. Individuals and organizations could both lose valuable capital and credibility. In addition, the theft of sensitive data could threaten Libertarian values as an invasion of privacy. Even the systems position is offended by computer systems which cannot be easily rendered secure. Nevertheless, security measures may compromise the Populist position insofar as increased security requires more complex procedures for ordinary people to verify their identities when transacting with EFl components. Unfortunately, many EFl advocates minimize the problems of large scale theft when they are addressing lay audiences who are satisfied with the current payments.
systems[1,8,11,25].

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.

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 EFDs rival the airline

* One may also buy reliability with backup equipment such as extra processors, core, and secondary storage. The costs of reliability increase accordingly.
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[16].

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 PJS as the medium for doing his business and such an error occurs while he is on a weekend trip, he may suddenly find himself unable to buy gas, food, or pay for his hotel**. Or consider the

** 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.
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 EFls. 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?

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 EFls? This is the kind of question that computer and banking professionals should be thinking through when they consider the technical feasibility of EFls.

* See [18] for a scheme to sabotage a real-time POS network.
Reliable EFT components are consistent with all the value positions discussed in this paper.

C. Privacy of Transactions and First Amendment 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 check writer.) 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 EFls, 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.

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

* 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 [9]. The court held in favor of the U.S. Government.
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 ACPS. 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 1975. Such a search could take several evenings of computer time and be unobtrusive*. In the current

* 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 defendant.
system, such a search would take an army of clerks several months and would be quite public.

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 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 "attendant costs" are less tangible than the dollar gains to be realized by ACPS beneficiaries.

Clearly, these privacy issues are most troublesome for the libertarian value position. In contrast, the statist value position is most served by weak privacy regulations. And the Free Enterprise position gains and loses. Keeping records inessential for business purposes costs money; informing data subjects when another organization accesses those records also eats into profits. Lastly some businesses may benefit from the increased data pools provided by EFIs when they wish to check the backgrounds of potential employees or customers.
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 [30, 31]:

1. "the sheer amount of meaningful personal data available on those with whom the system must deal [31];"

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 [31];"

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' [31];"

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."

Any of the major EFTs 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, on occasion, 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 EFT that would handle all of the society’s financial transactions.

Of course, such a proposal seems more consistent with our understanding of social control in the Soviet Union than in the United States. That such a proposal is so inconsistent 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."

Threats of political surveillance largely pit Statist against Libertarian values. However, the EFTs that enhance the surveillance potential of government agencies, such as the IRS or FBI, may be built and operated by legitimate businesses for their own economic gains. Both the IRS and the FBI, for example, may make routine and legitimate uses of financial data or data about the travels of people who
transact business through EFIs. The tensions center on what kinds of restraints on such access can inhibit abuse without rendering the legitimate activities of such agencies ineffective. To the extent that additional regulations hamper such agencies or place additional recordkeeping burdens on businesses that collect such data for private purposes, they will not be welcomed by either. This fosters a latent coalition between publics aligned with Free Enterprise and Statist positions who view EFIs as different kinds of positive resources.

E. Consumer Protection

EF1 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 Association has commissioned several market studies of the ease with which people would accept EF1 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 EFI 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 EFI 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 EFI 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, EFI advocates seem to be paying more attention to "marketing" EFI technologies than to designing them so that they will more adequately meet the felt needs of consumers[33]. 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

* A scheme for correcting erroneous billings is part of the California ACH operation, but this only covers pre-authorized payments rather than the ad hoc payments which characterize most consumer purchases.
systems. One simple and suggestive scheme is sketched in [18].

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

Simply labelling this issue "consumer protection" emphasizes the conflicts, rather than the common interests, between consumers and businesses. In our terminology, it pits the Populist position against the Free Enterprise position. Similarly, to the extent that people lose their choices in handling their financial transactions, the Libertarian position can also be compromised. None of these value positions are absolutes; rather there is an interplay between the interests which are most congruent with each of them. Different EFT arrangements can simply exacerbate the tensions between these positions.
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(4). 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 ACHS 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 arrangements are still unresolved. The National Commission on Electronic Funds Transfers includes representatives of the major classes of banking institutions, and its pluralistic composition suggests that no class of institution wiped out. In addition, maintaining maximal competition seems to be the primary concern of the Justice Department relative to EFT developments[5]. However, many bankers close to EFT developments sense that, generally, the larger banks will fare much better in whatever EFT developments emerge and that smaller banks may simply be unable to both compete and retain their independence. The results of the new competitive balance in an EFT dominated payments system most directly impacts the Free Enterprise position and latent conflicts between that position and the Populist position.
In the last two sections we have surveyed a number of major benefits provided by EFls to some parties and problems posed by EFls 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, EFl developments are most consistent with the Free Enterprise, Statist, and Systems positions. They come into greater conflict with Libertarian, Populist, and Conservative 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 EFl technologies exacerbate conflicts between these positions there are really no simple "public interest" arguments regarding EFl 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 technologies, such as multi-level freeways which crisscross the larger American cities, are, at best ambiguous, in their long-term consequences. As a culture, we are beginning to realize that the technologies we create may raise
subtle, unforeseen 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 DVI which may be banned by the FDA or communication satellites 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 National Commission on Electronics Funds Transfer Systems operating within Congress, but it is an advisory body which has just completed its deliberations[27]. These may result in appropriate legislation 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 surprisingly, the relevant government agencies and major private enterprises have more expert and widespread representation than do consumers or unconventional and thus disenfranchised political

* 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.
groups.

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 it 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 public 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...[24]"

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[26]. 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 debits and credits. 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 strongest in our present day environment[24]." 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 about inevitability obscure both the mad scramble of financial

* 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.
institutions for preferential market positions behind the scenes and our ability to choose which EFI technologies we want and how we want them. In the short run, active EFI development in 1977 undermines the proposals of the National Commission on Electronic Fund Transfers to help resolve some of the latent conflicts which are easily exacerbated by EFI developments (Commission). Active development and implementation of major EFI 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 EFIs in a way that deals with long-term problems that may be faced by many instead of short term gains accrued by the few.
 Bibliography


2. Armer, Paul Private Communication November 1975


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


