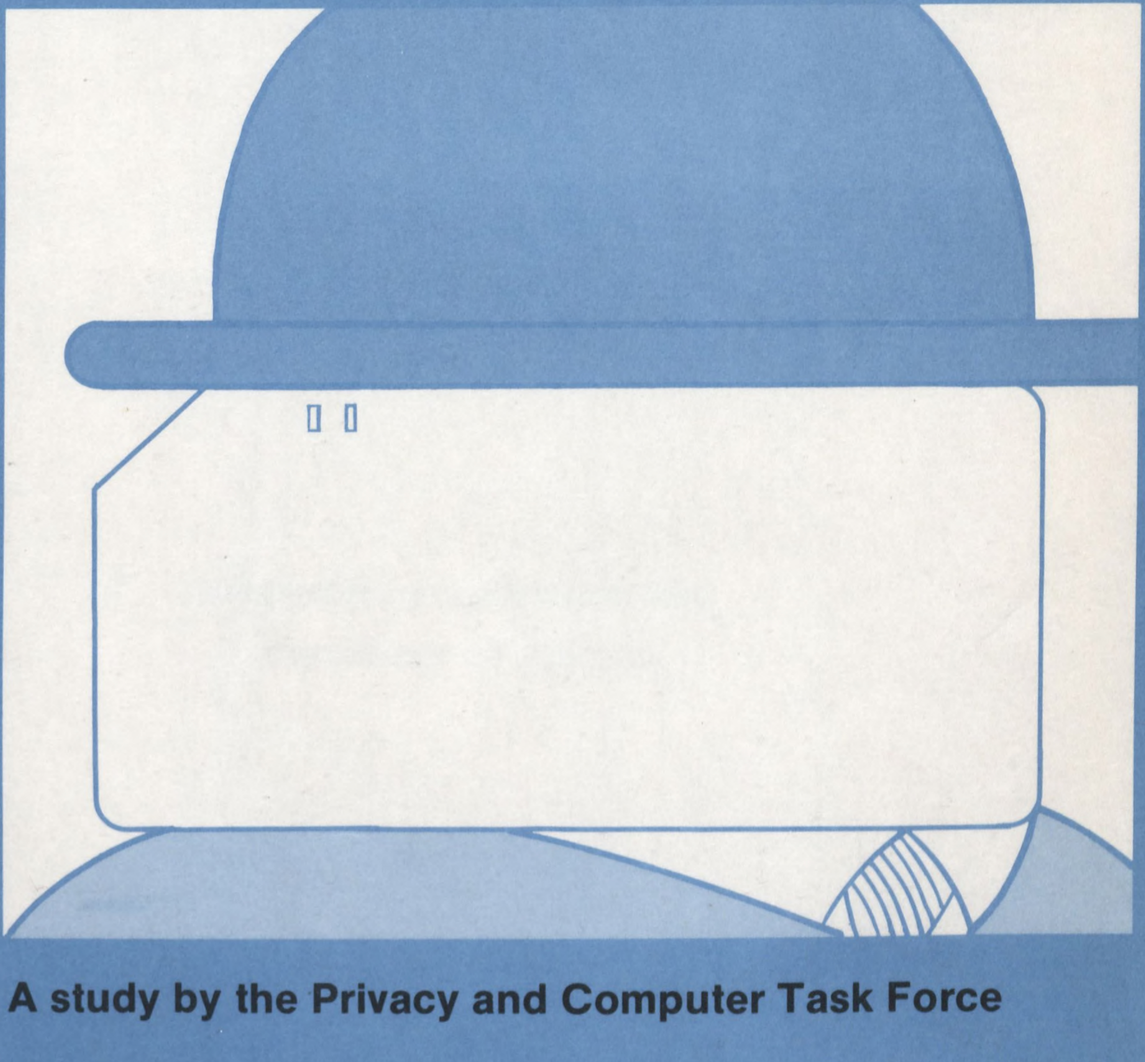
ELECTRONIC BANKING SYSTEMS AND THEIR EFFECTS ON PRIVACY

H.S. GELLMAN



9. A study by the Privacy and Computer Task Force

new

ELECTRONIC BANKING SYSTEMS AND THEIR EFFECTS ON PRIVACY

A STUDY FOR THE
PRIVACY AND COMPUTERS TASK FORCE

DEPARTMENT OF COMMUNICATIONS
DEPARTMENT OF JUSTICE

H.S. Gellman

This report was prepared for the Privacy and Computers Task Force, an inquiry sponsored by the Departments of Communications and Justice, and should not be construed as representing the views of any department or of the Federal Government. The views expressed herein are exclusively those of the authors, and no inference of any commitment for future action by any department or by the Federal Government should be taken from any recommendations contained herein.

This report is to be considered as a background working paper and no effort has been made to edit it for uniformity of terminology with other studies.

TABLE OF CONTENTS

ELECTRONIC BANKING SYSTEMS AND THEIR EFFECTS ON PRIVACY

I. INTRODUCTION

During the past two decades, banking systems in North America have been undergoing rapid evolutionary changes. One cause of these changes has been the advent of computer systems to process the growing mass of cheques and other documents.

At the same time, there has been a widespread adoption of credit cards, bringing significant effects on the spending patterns of people. In recent years, some of the major banks in Canada introduced the Chargex credit card, thereby increasing their involvement in the financial affairs of Canadian citizens.

Most of the banks and trust companies in Canada are expanding their use of computer systems, and some of their plans are very ambitious. For example, before 1975, the Bank of Montreal expects to have a comprehensive computer communications network connecting all its branches to a large-scale central computer facility. The plans of some of the other large Canadian banks are almost as comprehensive. By 1977 it is estimated that up to 75% of all the branches of Canadian banks will be connected to on-line systems.

These developments have caused some citizens to worry about being faced with a "chequeless" or "cashless" society in which all their financial transactions will be under the control and scrutiny of computer systems. Some individuals have had painful experiences as a result of errors produced by computer billing systems; others have had their credit ratings adversely affected by computer errors.

The increasing use of computer systems by the banking industry could lead to invasions of personal privacy for a number of reasons. First, it might become increasingly difficult to ensure the accuracy of data stored in central computers if a large number of bank tellers and retail store clerks can feed data directly into the computer through remote-access terminals. This inaccurate data could produce errors in an individual's financial account that might affect his credit rating. Secondly, if banking systems make more use of telecommunication facilities, more individual bank personnel might have access to confidential information through computer terminals, and this could make it more difficult to prevent disclosure of confidential information.

On the other hand, the banking industry in Canada has earned a well-deserved reputation for processing data accurately and for preserving confidentiality. This assurance of confidentiality is an important basis for success by the chartered banks. It could, therefore, be argued that the banking industry will probably continue to protect personal privacy in future, despite the new problems posed by increased banking automation.

It is, therefore, useful to examine the possible effects on privacy of existing and future electronic banking systems. The purpose of this paper is to describe some existing systems and suggest how they might evolve in future. An attempt will be made to identify potential invasions of privacy by these systems, and to suggest some possible safeguards.

II. EXISTING SYSTEMS

1. Bank Cheques

At present, the most usual way to transfer money is through the use of bank cheques. This method has gained such widespread acceptance that it has created massive paper-handling problems for the banks.

In 1967, Canadians used about 1 billion cheques, which is equivalent to about 3,250,000 per business day. This amounts to about 50 cheques per person in 1967 and compares with 22 per person in 1950 [1], when most companies paid employees in cash and credit cards were almost non-existent.

In 1969, Canadians wrote 1.25 billion cheques [2]. The growth rate of the number of cheques used in Canada has been averaging about 7% per year. This rate of growth is expected to continue until about 1980, then level off and start to decline [3].

It has been estimated that each cheque in the national banking system is handled an average of 14 times at a cost to the bank of 13 cents to process, with an additional 12 cents if an extension of credit is involved [4]. Significant potential cost reductions could, therefore, be achieved if the method of monetary exchange were simplified.

The banks have used computers during the past decade to speed up their processing of cheques. In Canada, automation in banking started in 1963 with the use of high speed sorting machines and specially imprinted codes on cheques. These sorting machines read the codes (Magnetic Ink Character Recognition or MICR), sort the cheques by account number and feed the information (account number and amount) directly into a computer, which produces the customer's monthly bank statements.

At present, about 60% of the branches of Canadian chartered banks are using computers (in the process described above) for demand deposit accounting for current accounts and personal chequing accounts. For savings accounts, about 450 branches of Canadian chartered banks and trust companies use specially designed keyboard terminals that are connected to central computers by telephone lines [5]. These on-line savings systems perform only a few functions such as recording deposits and withdrawals and updating the customer's book.

At present, Canadian banks are spending about $70 million a year for electronic data processing systems. This cost is for the equipment, personnel and supplies associated with the computer systems, and amounts to between 1.5% and 2% of total operating revenues. The current total expenditure in Canada for electronic data processing systems is estimated to be about $1 billion per year, so that the banking industry accounts for about 7% of the total [6].

Computers have helped speed paper but they have not reduced the amount of paper in the banking system. During the past fifteen or twenty years, systems designers have been arguing that the best solution to the money transfer problem is to bring the computer right into the transaction. Paper could be eliminated entirely if terminals — all linked to bank computers — were installed in stores, homes and offices. A transaction in this kind of system would involve merely the entry of information on the keyboard of a terminal or a Touch-Tone telephone. This system would also involve the use of a bank credit card or "money" card.

2. Credit Card Systems

The use of credit cards has received a lot of publicity and many people have thought that this was the road to the "chequeless" or "cashless" society. However, at present, the credit card is merely a substitute for money.

In the competitive credit-card industry, statistics are hard to get. Some rough estimates have been made [7] for the

United States. There are about 300,000,000 credit cards now in circulation, and about 100,000,000 are being added each year.

In addition to the petroleum-company card and the department store card, there are two major forms of credit cards in use today: the travel-and-entertainment (t&e) card, and the bank card. There are several differences between the two. A potential cardholder must apply for the t&e card; he must meet certain income and credit criteria; and he must pay an annual fee for the privilege of having the card. The service establishments he frequents pay the card company a percentage of their sales, and the customer is expected to pay his bill when it comes, although he may make deferred payments, with interest, on some large items such as air travel.

The giants of the t&e business are Diners Club, which was founded in 1950 and which now has about 2,000,000 cardholders; American Express, which started using cards in 1958 and which has around 3,000,000; and Carte Blanche, which started in 1959 and which has around 725,000.

The bank cards are more recent. There is no annual fee involved. As with the t&e cards, the participating merchant pays a percentage of his sales to the issuing bank. But the issuers make money from another important source: if the customer does not pay his account on time, it becomes an installment loan.

In Canada, the Chargex card was introduced in 1968. It is a joint venture operated by Royal Bank of Canada, Canadian Imperial Bank of Commerce, Toronto Dominion Bank and Banque Canadienne Nationale.

During the first nine months of 1971, national purchases through the system were 57% above the comparative period of 1970. Some important accounts have signed with Chargex recently. They include Gulf Oil Canada, Texaco Canada and several junior department store chains.

Chargex's total number of merchant accounts was 52,391 at the end of 1971, compared with 35,198 a year earlier. Many of these merchants have more than one retail outlet; some have hundreds.

The number of active cardholders showed a slower growth, rising by about 4.8% to 2.2 million. One reason for this is that Chargex has been purging inactive customers from its lists, to reduce overhead costs. Another reason is that Chargex has been forced to become more selective in adding new names to its lists. The service began operations by "blitzing" a region with direct mail. Many jurisdictions no longer allow firms to send out unsolicited cards.

In 1971, Ontario accounted for more than 41% of Chargex purchases, Quebec and the Maritimes 40% and Western Canada 18% [8].

In the United States, the banking industry has predicted that in the next five years more than 40,000,000 people will be using bank credit cards to make $15 billion worth of purchases each year [9].

Credit card systems do not reduce the volume of paper — they increase it. And paradoxically, they increase cheque volume too. Charles A. Agemian, executive vice-president of Chase Manhattan Bank argues that credit card sales replace cash sales, and the bills are eventually paid by cheque [10].

While cash is anonymous, credit cards are discrete and personal. They leave a trail of a person's activities, a record which can be examined and checked. Credit cards are a great convenience, but they do leave a person open to scrutiny since many of his financial transactions are recorded.

3. Direct Fund Transfers

Most large banks have been performing payroll computations for companies for years. The banks still produce pay cheques, but in a growing number of cases they are depositing the funds directly into the employee's account in that bank or another bank. This procedure reduces the number of cheques required and also cuts out a few steps in the fund transfer procedures.

A survey conducted recently by the Canadian Computer-Communications Task Force [11] indicates that many companies in Canada are thinking about moving to direct fund transfers. The Department of Supply and Services in Ottawa is currently considering the use of direct fund transfers to pay the members of the public service. In the United States it has been estimated that payroll fund transfers are made for only about 4% of the population, mostly senior executives [12].

4. GIRO Payment Systems

Giro payment systems are used in most West European countries and Japan. This type of system works in the opposite direction to our cheque payment system. The word is derived from the Greek guros, meaning ring, which conveys the circular concept [13].

In our present cheque payment (debit transfer) system, we generally mail a cheque in payment of a product or service to the seller, who then takes it to his bank for funds. The cheque is moved among banks until it reaches the buyer's bank. In making a giro payment, the buyer advises his own giro office (which is often a post office rather than a bank) to transfer funds from his account directly to the seller's account. This is the reverse of our present payment system, and is often called a reverse transfer, direct transfer or credit transfer system.

At present, about 44 countries have giro payment systems [14]. During the past three years, in Great Britain both the post office and the banks have installed new electronic giro systems [15], [16].

Giro payment systems can provide cost advantages over our present payment system. A seller would obtain payment more quickly than at present. Both commerical and consumer buyers would save on accounts payable paperwork and postage because they would not have to prepare and mail separate payments to different companies. Sellers and buyers would have lower bank charges as a result of eliminating much of the physical handling of cheques.

The success of the giro systems in Great Britain has helped to generate interest in this type of system in the United States. George C. White Jr. of the Irving Trust Company in New York City [17] has advocated the installation of a giro system in the United States, and has discussed its feasibility. Kramer [18] has suggested that progress toward a giro system in the United States will be slower than in Great Britain for several reasons:

- The United States does not face a government-sponsored giro system.
- The task of coordination is far more difficult in the U.S., which has more than 14,000 banks compared with about 24 in England. American banks range in asset size from under $100,000 to more than $15 billion.
- There appears to be less room for improvement in the U.S. system; for example, the typical credit transfer takes two days there as against four days in England.

Until now there has not been any strong movement in Canada toward a giro system. It is possible, however, that Canada will end up with such a system in future if the use of direct transfer payments increases.

5. Preauthorized Payments

A significant potential for reducing the amount of paper to be processed is available through the use of preauthorized payments. In this system, customers give their banks standing instructions to pay recurring bills automatically. Life insurance companies have used this system for years and some banks in the United States have been developing similar programs with electric utilities [19]. The Canadian Post Office recently did an environmental study which led to a prediction that by 1985 there will be a 10% reduction in first class mail volume because of an increased use of preauthorized payments [20].

6. Computer Services Offered by Banks

Most of Canada's chartered banks offer computer services to some of their customers. The most typical services today are: account reconciliation, payroll preparation and labour distribution analysis. One bank is providing billing services for doctors.

In future, the banks may expand their computer services to customers, for several reasons. First, banks are finding it more difficult to maintain the level of income they receive from money on deposit. The turnover of funds is increasing as people learn to make better use of their money and avoid letting it sit idle in a bank account. The ratio of the value of cheques cashed to the average of deposits has increased from 65.29 in 1961 to 116.31 in 1970 [21]. To counteract this reduction of income from money on deposit, the banks will have to obtain revenue from other sources. They may develop new computer services to provide some of this revenue.

Secondly, as the banks progress in the development of more elaborate computer systems to serve their own needs, they will be able to offer a wider variety of computer services to their customers. Thirdly, banks can afford to make large investments in computer systems. This will enable the banks to achieve larger economies of scale than other computer service organizations can. Fourthly, the banks have an existing branch office system that can provide a powerful marketing and distribution system for new computer services.

Some of the non-banking, computer services that the banks are likely to provide in future are: billing and accounts receivable, accounts payable, sales analysis and inventory accounting. Thus, there may be a significant accumulation of information in a bank, concerning its customers' operations.

7. On-Line Banking Systems

At present in Canada, there are about 450 branches of chartered banks and trust companies that have remote-access computer terminals that enable tellers to process deposits and withdrawals automatically for savings accounts. About 300 of those branches are in Toronto, 150 are in Montreal and Quebec City [22]. Hence on-line banking is concentrated at present in the large cities.

None of the Canadian banks are currently using on-line computer systems for current accounts or personal chequing accounts. The Bank of Montreal is developing a comprehensive on-line system which will link most of its 1,100 branches from coast-to-coast with one centrally controlled computer system. The system will handle nearly all banking transactions. Each branch is to have its own on-line terminals.

The Bank expects the first terminals to be installed during 1972 and the complete system to be operational by January 1, 1975.

The Bank of Montreal expects to improve the efficiency and economy of its existing operations while providing better services, at lower costs, to its customers. As a by-product it expects to obtain a powerful and effective bank management information system.

It intends to provide a better funds transfer facility, as well as a number of specialized banking-related data processing services to its banking customers across Canada [23].

Other Canadian banks are also developing large scale on-line computer systems to handle most of their banking functions. Adams [24] has estimated that by 1977, 60% to 75% of Canada's 6,200 bank branches will have on-line computer terminals for handling savings accounts, current accounts, personal chequing accounts and various other banking transactions.

8. Problems with Existing Systems

The problems to be discussed here will be only those that relate to the disclosure of confidential information, the invasion of privacy or the restriction of a person's freedom of action.

(a) Credit Card Billing Errors

When a person acquires a credit card, he gives up some confidential information about himself, in exchange for the convenience offered by the use of the card.

On occasion, however, the apparent convenience of a credit card turns out to be illusory. Some individuals have been subjected to long, annoying arguments with companies whose computers have made billing errors. One example is the case of a lady who received a bill for $369.78, plus interest. The lady claimed she did not purchase anything from the store. The store threatened to sue her. The matter was finally settled, but the lady believes that the store damaged her credit rating with other stores [25].

A second example, reported recently in Computerworld [26], is the problem encountered by a man who never had an oil company credit card, but the computer has been sending him bills and dunning letters for the past year. The man wrote several letters to the credit department, but none was answered. He is quoted as saying: "What bothers me is that I get no response. It is as if I was not writing to anyone at all."

A third example concerns a man in the U.S. who made a purchase in December, 1969 for $12.71. The credit card company billed him double that, or $25.42. He paid the $12.71 and attempted to explain the mistake.

The following month he was billed for the remaining $12.71 and 50 cents interest. Finally, in June, he was credited for the overcharge but billed for $1.50 in unpaid interest.

The man called on his senators and congressman for help. He also borrowed $150 on the credit card and announced he would return it when the $1.50 charge was removed.

The credit card company settled its difficulties with the man by sending him a cheque for $10 and explaining, "Seemingly, there is no solution" when billing computers go awry. The man responded by stating that the $10 did not come near covering the expenses he incurred in the battle. He added that he did not accept the explanation offered [27].

Ralph Nader has discussed the question of what a citizen can do about a department store computer that makes mistakes [28]. He states that:

> "There is no general answer, except that the department store is the problem and not the computer. We need complaint centres manned by citizens. One has been set up in Cleveland, which is manned by students. It has had much success in solving complaints. Computer abuses hit everybody; they are not discriminatory; but they are traceable to the managerial system operating the computer."

Although computer system errors at the credit card companies are common knowledge and are not rare, local and regional credit bureaus reportedly accept, on a routine basis, whatever information credit card companies give them. As Boeth [29] has suggested,

> "Once the deadbeat mark goes down against a citizen's name, it stays there, following him from state to state, summonable in as little time as fifteen seconds from the memory banks of the computers. What isn't summoned is the all-too-frequent explanation — that somebody mixed up two names or forgot to record a payment, or that the computers went bonkers."

Milton T. Pearson, general manager of Associated Credit Bureaus of Canada, has said that moneylenders have no way of knowing, despite their exhaustive files, the true state of a man's financial affairs. He feels that a strong, central index is necessary and that this should have access to information that is protected by law at present [30]. For example, the credit bureau files do not reveal a person's indebtedness to the banks. The Bank Act guarantees this privacy. Thus, a loan company may check a person's records, find them unblemished, advance the requested $1,500 only to find the borrower declaring bankruptcy three weeks later.

In the United States the Fair Credit Reporting Act took effect April 25, 1971. This act provides some protection against the harm done by inaccurate or outdated information in credit files.

Under the new law, if a person is refused a job because of a credit or investigative report, or he is refused or charged more for credit or insurance because of such a report, the company using the report must tell the person. He then has the right to ask the reporting agency to show him the contents of his file without charge. If thc individual disputes the accuracy of an item in his file, the reporting agency must reinvestigate that item.

The law also makes provisions for dealing with investigative reports, which frequently include interviews with "enemies" and neighbours and which are commonly used when a person applies for a job or insurance. Under the law, a person must be informed of such an investigation within three days after it is requested (31).

Other federal regulation has also been proposed in the United States. A bill sponsored by Senators Proxmire and Brooke would, among other things, prescribe new billing criteria, set forth the method by which banks and other revolving-credit operations calculate monthly interest charges and require that bills be mailed out to customers at least twenty-one days before payments are due. In a recent article, Ross (32) indicates that the U.S. banks take a dim view of these "consumerist" initiatives, regarding them as unnecessary and cumbersome, as well as costly.

In April, 1971, the Ontario Government introduced legislation to regulate the collecting and reporting of information by credit bureaus. As of the beginning of December, 1971, this legislation had not yet been passed (33).

The legislation would make the following changes in the practices of credit bureaus that gather information for consumers' credit ratings:

- bar credit bureaus from collecting information about the personal habits and morals of individuals, as well as unsubstantiated rumors about individuals;
- direct credit bureaus to destroy after specified periods of time all information harmful to an individual's credit rating;
- provide ways for individuals to correct wrong information about them in credit bureau files;
- require retailers to inform individuals, upon request, that they are being refused credit because of information received from a named credit bureau.

All credit bureaus or credit reporting agencies, as they are referred to in the legislation, will have to register with the provincial government. They will have to store all their information in Ontario.

They will be liable to fines of up to $25,000 if convicted under the proposed legislation.

The legislation falls short of meeting some of the demands for reforming the collection of credit information.

- It does not require credit bureaus to inform individuals automatically that a file on them exists. An individual must approach a bureau and ask if such a file exists.
- It also exempts the credit departments run by department stores and other retailers for their own use.
- It imposes no restrictions on the use of credit ratings for investigative purposes by prospective employers, insurance companies and other non-retail establishments.

In commenting about the proposed Ontario consumer credit reporting bill, Professor Ziegel [34] welcomed the bill as an indication of the government's willingness to come to grips with an important problem, but feels that the bill is seriously defective in a number of important respects. He urged the establishment of a standing advisory committee on consumer reporting agencies to be made up equally of consumer representatives, independent experts and representatives from the industry in order to improve the proposed legislation.

(b) Preservation of Confidentiality

In today's banking systems, apart from any involvement with electronic systems, a customer cannot always be certain that confidential information about himself or his financial affairs will be fully protected. The banks treat confidential information with great care because they realize how important it is to retain the trust of their customers. However, a number of cases have been cited where confidential information has been disclosed.

Breaches of confidence have reportedly occurred when inexperienced junior bank personnel gave out confidential information over the telephone, without realizing the seriousness of their actions. In Great Britain, Mr. Kenneth Baker, MP, interviewed on BBC radio in February, 1969, revealed, in the course of the program, that there are investigative agencies that will undertake, for a suitable fee, to discover anyone's current bank balance accurately to the last penny, within twenty-four hours [35].

When a person applies for a bank loan, he usually divulges an extensive set of facts about his personal and financial affairs. Of course, he does this as a necessary condition for obtaining a loan, but he has no way of knowing how many "eyes" within the bank may get to see this information, nor can he be certain that someone outside the bank will not get to see it.

If the data security procedures associated with the banks' computer systems are not adequate, confidential information could be disclosed. Jacobson [36] has reported that during a test of the security of a large eastern computer centre, a stranger found that he could enter the computer room and sit down in front of the console without attracting the attention of the dozen or so people in the computer room. Worse than that, he was able to walk into the tape vault and remove a tape from the computer centre!

The author knows from his own experience that, about a year ago, one Canadian bank had such inadequate security procedures for its computer centre that a bank security officer was able to enter the computer room without being challenged. The security officer carried a pencil and pad of paper, and was apparently assumed to be a member of the programming staff.

The security procedures in that particular bank have now been significantly improved. Moreover, the author is aware that most of the Canadian chartered banks are spending a lot of time, effort and money on improving the security of their computer systems.

Although considerable work needs to be done to provide adequate security for a computer system, it is likely that a "secure" computer system will protect confidentiality better than the manual system it replaces. The reason is that security procedures for a computer system are largely automatic, leaving less opportunity for human error.

(c) Credit Card Fraud

Fraud is a peculiar affliction of the credit card, simply because the card is a highly portable item of great potential value that commands an endless array of merchandise, much of it readily convertible to cash. Credit cards are lifted by pickpockets but the largest supply of stolen cards has come right out of the mails [37].

Cards intercepted in the post before they reach the addressee are highly prized, for they have not yet got the cardholder's signature and hence can be fraudulently used without arousing any suspicion of forgery. According to Eugene Gold, who is District Attorney of King's County (Brooklyn), New York, about 1,500,000 credit cards are stolen or lost each year [38]. Gold estimates that fraud losses from credit cards which ran about $20 million in 1966 were up to more than $100 million a year in 1969.

Milton Lipson, the vice-president in charge of corporate security at American Express, is proud of his computers and especially proud of their ability to plot a cardholder's spending habits over a period of time, sort the information and spit it out when needed. With a staff of 300, Lipson manages to keep American Express's fraud loss down quite low, the lowest ratio in the industry, he thinks [39]. All this is quite necessary, he feels, "inasmuch as the attacks on credit cards, as the attacks on anything of value, 'run the gamut of the imagination of man'."

The same computer system that is used to track criminals who are using stolen credit cards can be used to keep track of a law-abiding cardholder's travel and spending patterns, and this would constitute an invasion of privacy. As Henderson [40] has suggested:

> "Credit cards establish...where we eat and shop and how much we spend. In the cashless society to come, even the smallest transactions may be fed instantly into central computers to put every detail of our daily life on record. If you knock off work mid-afternoon to take in a movie or go out to the golf course, that tiny transgression may be irrefutably noted when your account card is processed at the box office or club house."

In a similar vein, Westin [41] has written:

> "Another disturbing fact in this prospective universal credit system is that the life of an individual would be almost wholly recorded and observable through analysis of the daily 'transactions' of 'Credit Card No. 172,381,400, Humphrey, Stanley, M.'. Whoever ran the computers could know when the individual entered the highway and where he got off; now many bottles of Scotch or Vermouth he purchased from the liquor store; who paid the rent for the girl in Apartment 4B; who went to the movies between two and four P.M. on a working day at the office; who was at lunch at Luigi's or the Four Seasons on Tuesday, September

> 15; and the hotel at which Mrs. Smith spent the rainy afternoon last Sunday".

Rogers [42] has described a cashless chequeless system that is currently being tested in Ohio. He writes, "All month the computer 'follows' Mrs. Seeling whenever she shops with a participating merchant and at the end totes up her bill and mails it to her."

The procedures required to prevent credit card fraud constitute a further potential invasion of privacy since individuals will have to carry what amounts to an identity card including an identifying number, signature and photograph.

(d) Computer Fraud

Each year, millions of dollars are embezzled from corporations. In an increasing number of cases, computers have been used, either directly or indirectly, to commit fraud. The problems of fraud prevention and detection are quite complex in today's computer-based systems. In tomorrow's computer-based systems, which will be more elaborate than today's, the problems of fraud prevention and detection may become even more difficult to solve.

Until quite recently, there were sharp differences of opinion as to whether the computer might become directly involved in fraud. Some authors vigorously maintained that computers were not involved [43]. It is not surprising that it is difficult to cite specific examples of computer fraud because it is a characteristic of this problem that all parties related to a particular fraud have little to gain and much to lose from publicity. As a result, fully documented cases are rare and in those infrequent instances where information is given to the public, it is often very brief.

There is sufficient data, however, to conclude that computers have been involved in fraud schemes. For example, employees in one office of E.F. Hutton, a prominent brokerage firm, raided customer accounts of more than $500,000 and when the customers complained of the shortages indicated in their computer-printed statements, they were mailed apologies that essentially said: "Don't worry. We are having trouble with our computer. We're sure you will understand." And their customers did. The scheme went on for months [44].

Another example is the case of a programmer in a bank who altered the savings account program to transfer the "round-off" fractions of cents in the interest calculation to an account he maintained under a fictitious name; he was able to withdraw large sums of money before his scheme was detected [45].

Another case, which the author encountered in his consulting work, involved a Canadian chartered bank. Funds were stolen from the bank by an operator of a cheque sorting machine. The operator was able to forge cheques, intercept them during the sorting procedure and arrange to have the appropriate control totals balance properly.

A programmer in a bank managed to steal large amounts of money simply by programming the computer to by-pass his account number when reporting on overdrafts. He was then free to overdraw his chequing account by any amount he pleased [46].

Although Canadian chartered banks are continually improving their data security procedures, the potential for computer fraud still remains, and it may increase as the computer systems in banks become more complex. Man seems to have the ability to commit criminal acts no matter how difficult the circumstances — he escapes from escapeproof prisons, tampers with tamperproof devices and burglarizes burglarproof establishments. No level of technology has found itself above the ingenuity of a clever mind.

Although computer fraud does not usually affect individual customers of a bank, the methods used to steal money from a bank can also be used to steal information, and this could lead to disclosure of confidential information and invasion of privacy.

(e) Cheque Forgery

A recent article in the Toronto Star [47] indicates that the number of forged cheques which have been cashed during the past year is double the rate of five years ago. So far this year, swindlers have robbed at least 200 of Metro Toronto's 1,300 mail boxes. That is almost 1 in every 6, a good measure of the scope of the racket.

Recently, two food chains have begun experimenting with a new computer system called "Approve-a-Cheque". This is a computerized version of the store supervisor's hurried initialling of cheques presented by customers for goods. Under the experimental system, cheques can be cashed only by a customer who has registered previously with the computer system. The customer completes a card with personal details, including the usual credit information, such as a personal bank account number, place of employment, driver's licence number and credit references. Once approved by the store's credit service, which may take a week or so, the customer can use the system.

The customer gets a card carrying a coded number and a code word — the word created by the customer herself and known only to her and the computer. To pay by cheque, the customer inserts the card into a computer terminal and, if the computer finds it valid, the machine writes "Approved" across the cheque. Every year stores that offer cheque-cashing privileges pay heavily for the cost of this service because of dishonoured cheques, or rather their customers do. The companies are remaining cautious about the new system until they can check that it works reliably and until they can assess customer reaction. They stress the time-saving aspect of not having to wait around for a busy supervisor each time a cheque is presented. But there is no doubt that they are also very interested in anything that can replace the present haphazard and costly system [48].

The above problems and examples demonstrate some of the potential adverse effects on privacy and freedom of today's banking systems. If the banks should develop more elaborate and more complex computer systems in the future, it is conceivable that these problems could become more acute. The author is aware that some Canadian banks are currently addressing, with considerable care, the problems described above. It is reasonable to expect that the banks will remain alert and will try to anticipate new problem areas. It is important to ensure that these problems are taken seriously and that complacency is avoided. As Osvald [49] has stated in his discussion of a proposed banking computer network in Sweden,

> "We think that it is important to realize that security problems — in the broader sense of the word — with the introduction of an integrated payment system and a public datanet in combination will assume quite new and critical dimensions. As a general rule I think that security problems, systems as well as technical, have been overlooked to an extent that is possible in more limited, intraorganizational systems, but now absolutely must find solutions that are considered satisfactory also and above all from a public interest standpoint. The success or failure of the payment system as well as the public datanet may be a question of whether the security problems are solved or not."

III. POSSIBLE FUTURE SYSTEMS

It is impossible to predict the precise sequence of future events. It is, however, often useful to speculate about the probable features of future "scenarios". This kind of speculation can be helpful by providing a framework in which to think about potential future problems and possible solutions.

The primary impetus today for improving the payments mechanism stems from the recognition of the enormous cost of the rising tide of paperwork and the knowledge that there are other ways to move money besides preparing and exchanging documents.

Changes in the payment system will likely be evolutionary in nature, and it is possible that several different practical designs will exist for the future banking systems at the same time. But the underlying purpose of all the systems will be the same. The idea will be to harness the speed and massive information storage capabilities of modern electronic computers. One picture of a possible future system has been described by Kramer [50].

> "Joe Smith is travelling and needs some ready cash. He goes into a bank and presents an identification card (the only card he has to carry) to a teller, who puts the card into a terminal box. A green light appears. The teller punches a few buttons and hands Joe his money. Joe signs a receipt.
>
> Joe is not worried about the size of the balance in his bank account back home because the day before was payday, and his employer passed the funds through the wire transfer system to his bank. Joe also knows his money is 'good' money. Even if his wife has been drawing on their joint account, the bank (through a loan agreement) guarantees to place the necessary funds at his disposal.

> Let us examine Joe's card and find out why it possesses a genie's magic touch. There are several forms of identification on it. It carries the name of his bank and his identification number (each in both readable print and machine language); it also carries his signature and photograph and has an invisible (magnetically encoded) two-digit number. The two-digit number—generated, recorded, and stored by the computer at the time of the last transaction— serves as a password to allow access to Joe's account. After each transaction, a new number is generated and stored; a counterfeit card would not have the correct number encoded on it. (When Joe Smith's card produced a green light in the terminal box, the teller immediately knew that the money was available and the card was authentic. He looked at the tamper-proof photograph and signature and established Joe as the card owner.)
>
> Every few days Joe takes his machine-readable bills to a pay station on the corner. He calls the central computer exchange and inserts his identification card into a slot. A verification voice acknowledges him. One by one he drops in his bills, and the voice repeats instructions until the last bill has been processed. Joe is a shrewd man; he pays every bill promptly and obtains a discount, which shows up as a credit on his next bill. Joe knows the value of money and keeps ahead of the game, realizing that if an emergency arises, he may need to use his credit privileges to the fullest extent."

A system of the above type is currently being developed in Sweden [51]. The SIBOL Project is based on the use of a bank card that gives access to one's accounts in a bank computer via on-line terminals.

> "The core of the system consists of a communication computer or a computer exchange which functions as a marshalling yard for the entire payment system. In principle, all payment transactions must pass it on their way between the sender and receiver. The communication computer will be connected to the commercial banks' computers, the savings banks' computing centres, etc. as well as to teller terminals, retailer terminals, company terminals and even home terminals, and also connected to a number of support systems or files that are important for the function of the payment system, such as post-and bank-giro centres, credit card centre, credit information centre, the stock exchange, real estate data centre, the central bank of Sweden and the nation bureau of statistics."

In Upper Arlington, Ohio, 31 merchants, more than 2,000 customers and a bank are joined in a pioneering experiment that is aimed at moving toward a cashless chequeless society [52].

Says John Fisher, a vice-president of City National Bank in nearby Columbus, which directs the test using credit cards and a computer:

> "The typical customer pays for the whole month's business with just one cheque. In a normal month she would have written about 30 cheques and it is that sort of volume that is literally smothering U.S. banks under mountains of paperwork. American banks are processing 22 billion cheques a year and in 10 years that is likely to double. We just can't take it. The Federal Reserve Board has indicated that government might have to step in with new regulations if the banking industry can't develop some way to reduce the load."

The Upper Arlington experiment, which seems to be going well, is an effort to make that reduction. When a customer arrives at the checkout counter of a supermarket, she hands over her credit card that has special magnetic identifications. The clerk inserts it in a slot in a little keyboard and dials a phone number which connects the keyboard with the computer which is a dozen miles away in the bank. The computer, which already has identified the customer from her card, now verifies the amount of the sale and the fact that the customer pays her bills. And the sale is over. A normal transaction takes about 15 seconds.

The system has security features that reduce the danger of loss. For example, since the computer knows which customers have become deadbeats, if one of them tries to make a purchase with his credit card, the computer tells the store clerk and the card is lifted. Or, if the owner of a lost or stolen card calls the bank, the computer is notified within seconds. Then, if someone tries to use it, the computer rejects the sale and that card, too, is lifted.

Small shop owners, potential targets for robbers, are eager to cut down on the cash in their registers. And a number of housewives report that they feel more secure carrying smaller amounts of cash.

In his report on this system, John G. Rogers writes:

> "The merchants taking part in Upper Arlington's test represent about half the community's business. Others, and some customers, too, are leery of the experiment. Buyers are creatures of habits, suspicious of innovation...Some fear that credit cards will impel them to overbuy and some just resent the way society is becoming ever more organized, impersonalized and numbered.

> ...The best guess right now is that when the test period runs out in April, the project will be continued and extended to include more participants."

No one questions the technological feasibility of a nationwide computer information network. Several regional, national and even international computer networks are already in operation [53]. Touch-Tone telephones with attachments capable of reading information from plastic credit or identification cards are in use. American Airlines and American Express early in 1971 tested an IBM machine at Chicago's O'Haire Airport which accepted a specially magnetically encoded group of American Express and Air Travel Credit Cards which had been sent to a test group of Chicago cardholders who fly frequently. Within a minute, the machine ate up the card; asked the traveller which of eleven airports he wanted to fly to and whether he wanted to go first class or tourist; told him when the available flights where, and printed, bound, and spat out the completed ticket. The traveller could not get the ticket, however, until he remembered to retrieve his credit card. If he had made advance reservations for his flight, the machine worked even faster. All the safeguards against fraud were built into the machine [54].

Despite the availability of the necessary technology, major implementation problems remain in the areas of financing, education and marketing. In addition, some major technical problems remain such as choosing and applying a numbering system to identify system users, perfecting security protection systems and devices for preventing accidental or fraudulent transactions, satisfying legal requirements in government agencies, designing and programming the system, and standardizing subscribers' computer files.

There are those who foresee many difficulties and drawbacks, some perhaps insurmountable, along the way to the "chequeless" society. Some of these doubters question its economic justification. They point to recent improvements in the present systems, such as speeding up credit reports through computerized credit bureaus, automatic bill payment, direct payroll deposits, the growing use of credit cards, optical character recognition devices and improved paper handling equipment. But others see the "chequeless" society as financially feasible and of great benefit to our economic welfare. They see it as a logical evolutionary outgrowth of current trends in automation, banking and consumers' financial behaviour. In their view, the payments mechanism has evolved over the centuries and will continue to do so; the "chequeless" society is part of this change.

As a group, U.S. bankers themselves are somewhat pessimistic about the development of the "chequeless" society. A few years ago, a survey of them indicated that 53% regard the elimination of cheque writing as not likely to happen, another 32% feel it is at least ten years away. To a question on the paying of bills via telephone, the answers were only a little more optimistic: 25% believe it is not likely to happen and 39% feel that it is at least ten years away. On the development of a national uniform identification number, 40% of the U.S. bankers think it is at least ten years away and 19% regard it as not likely to happen [55].

Whether or not we achieve a "chequeless" or "cashless" society during the next ten to twenty years, it is highly probable that the use of credit cards will become more widespread and more firmly entrenched. It is difficult to foresee whether the bank credit cards in Canada will assume a dominant role in relation to the t&e cards and the department store and oil company cards.

The banking industry itself is split over credit cards. One of the Canadian chartered banks prefers to issue cheque guarantee cards in conjunction with personal lines of credit. Another bank uses a bank card cheque which works like a traveller's cheque and involves the use of a bank identification card.

Another stumbling block for the banks could be the fact that big department stores with their own credit cards have so far given no indication that they will ever agree to join bank card plans [56].

This last fact could prove an enormous stumbling block to the banks. The fact is that big department stores have a big banking business of their own going which they are not likely to relinquish easily. Retailers know there is more to their card plans than just interest rates. For one, cards give them an identity and image in the shopper's pocketbook. Secondly, retailers who care about customer relations do not want some cold snobbish banker in the middle if something goes wrong, and thirdly, they consider the information in their customer files pure gold for sales analyses and mail promotions [57].

Oil companies, on the other hand, are less reluctant to join bank card plans. Shell Oil Company accepts BankAmericard in California and Sunoco, Gulf and Texaco accept Chargex cards in Canada.

Mr. R.D. Fullerton, senior vice-president and deputy chief manager of the Canadian Imperial Bank of Commerce, recently forecast a move toward a single all-purpose credit card [58]. Mr. Fullerton stated:

> "We believe a single all-purpose card will have a strong attraction for all but those who, for whatever reason, prefer multiple sources of credit."

He added that:

> "An overall approach will be to continue to expand the facilities available under the Chargex card and tie it into the individual customer's total relationship with his bank."

Whether a single card will replace cash in the future in all but a few minor transactions, or whether a multiplicity of cards will remain, it is reasonable to expect that bank credit cards will play an important role. It is also reasonable to expect that during the next few years some small and medium retail stores might have remote-access terminals, owned by a bank, connected to the bank's central computer. Such terminals could begin to be used for credit authorization only. For example, today in Toronto, both Eatons and Simpsons use simple terminals with a small keyboard for input, and display lights for output, to verify the authenticity of their store credit cards. In the U.S. a major experimental point-of-sale system, Omniswitch, involving large corporations such as First National City Bank and several large department stores, was scheduled to go into operation in the fall of 1971.

It is also possible that in future, the bank credit card would have a magnetic tape on the reverse side bearing all necessary identifying data, that the clerk could insert the card into a terminal, key in the dollar value of the sale on a small keyboard, press a button and get a speedy response from the computer, an audio signal or a light signal authorizing the sale or declining it.

The next logical step would be for the computer simultaneously to post the item to the customer's account, obviating the need for the charge slip to be sent to the processing centre. Then, the terminals and computer could be programmed to debit the customer's chequing account or his card account while at the same time crediting the merchant's account. The credit card would thus also be a cash card. But the possibility of errors if the sales clerk taps out the wrong number makes people pause about the last step described above.

At that point, it would not involve much extra work to enter the stock number on the keyboard of the terminal. These steps would provide enough information to the bank's computer to enable the bank to offer a comprehensive information system to its retail customers.

The larger retail establishments might own their own terminals and computer networks and might exchange information with the banks, in summarized form, through the use of magnetic tape or other means.

Robertson [59] has predicted that in Great Britain, the electronic banking network will probably develop through the following phases. The first phase, which may take place around 1973, would have customers' accounts centralized at their banks' computer centres and an interbank computer bureau will exchange magnetic tapes with the various bank computer centres and accept tapes from some customers with their own computers. In the second phase to come in the middle 1970's, magnetic tape exchange will be replaced by data links. This will merge into the third phase, up to about 1980, in which government departments, industries and others will have created data networks of their own, which will be increasingly linked to the bank network and each other. By the middle 1980's, the separate networks will probably have coalesced into one national data network, like the present telephone network.

As the Canadian chartered banks expand their computer systems, they will be in a good position to provide additional computer services to their customers. They will be able to offer a wide variety of computer services related to financial information systems. The Commercial Letter of the Canadian Imperial Bank of Commerce in April, 1969, [60] states that:

> "As the big planned extensions to data processing capacity come into use, the banks will be in a position to offer a growing range of services tailor-made for individual clients by the banks' own staffs of systems analysts. These could cover such diverse functions as sales analysis, consumer analysis, order entry and analysis, account reconciliation, accounts payable, accounts receivable, production control, labour expense and distribution, and many others. They may even

> undertake to handle all the accounting for a business. This new form of activity would serve two very useful purposes. It would enable a bank to make more economic use of its computer investment while at the same time strengthening its over-all competitive position through diversification."

The Canadian chartered banks will be in a good competitive position compared to other computer service bureaus. The banks will probably have large resources in equipment and personnel. This will enable them to achieve significant economies of scale which they can translate into lower rates for their customers. In addition, the banks will already be providing standard banking services to these customers. Many customers will buy computer services from banks where they will refuse to buy similar services from other organizations. This is due to their belief that the banks have financial stability and can be trusted to preserve confidentiality.

Some bankers feel that the credit bureau business is a natural adjunct of their operations [61]. It is not unreasonable to predict that banks will enter the credit bureau business in future.

Some finance companies foresee such a possibility and are seriously concerned. They are afraid that if banks take over the credit file and information exchange field, it will be the first step toward eliminating loan companies altogether. Finance companies are already getting pinched by the banks' moves into consumer credit. The CIT Financial Corporation was one of the first to start hedging its bets. In 1965, it bought New York's Meadowbrook National Bank [62].

Professor Miller has described the TRW Credit data system which had computerized credit information on more than 20 million Americans in 1968 and currently has information on more than 50 million [63]. He mentions that the TRW Credit data base was secured by convincing several California banks to turn over their stockpile of California information; Bank of America alone supplied 8 million items. Miller [64] also states:

> "The increasing acceptance of credit cards has enormous significance. It may herald the first stage of the chequeless, cashless society in which the credit granting and credit rating industries might cease to exist as separate entities. Should this come to pass the accuracy of the records and the integrity of those who handle them will be matters of overwhelming importance to the individual's purchasing power. Thus, computerization, networking and reduced competition are bound to mire the credit information industry even more deeply in the morass of the privacy problem."

Mr. M. Cox, general manager of the Credit Bureau of Metropolitan Toronto, has stated [65] that computerized credit files will come within the next two or three years. The author knows that the Credit Bureau of Metropolitan Toronto has been discussing, for many years, the possibility of putting their files on computers. In view of their long delay in doing so and in view of the larger financial resources available to Canadian chartered banks, it is perhaps reasonable to speculate that in future the banks will have their own computer files of credit information. The banks might supplant the credit bureaus or at least provide them with significant competition.

Some of the possible developments described above may not be implemented as soon as some people have predicted, because there are a number of inhibiting forces that may postpone their implementation. One such force stems from the fact that many people still believe that paper has advantages in the transfer of money.

As Stiefel has suggested [66]:

> "At present, a transfer of property, such as writing a cheque, requires a signature, which is a very distinct action by the owner showing his willingness to transfer some of his property. In contrast, the mere pushing of a button or the insertion of a key does not constitute an equally distinct intent of the owner to transfer property. It can easily be claimed that a wrong button was pushed or a wrong number inserted, whereas the signing of one's name on a cheque is an action that cannot readily be renounced as having been committed accidentally."

Stiefel goes on to ask:

> "Are the 20 billion cheques that are expected in the United States in 1970 a sign of excessive paperwork and bureaucracy or are they a testimony to a very active society?"

He believes it is the latter, and that it bespeaks of the efficiency of the economy that values of hundreds of millions of dollars in effort, labour and material can be safely and adequately transferred with a piece of paper. He lists the following disadvantages of a piece of paper.

- It is maligned and unfashionable.
- The information content is difficult to alter.
- It is not easily machine-readable.
- It is not readily electrically transmittable.
- While most conveniently storable, it is not conveniently retrievable in automatic form.

In Stiefel's view, the following are some of the advantages of paper.

- It is human-readable.

- As one of the oldest information storage mediums, considerable skill has been accumulated in its use.
- It has a small volume since it is very thin.
- Two dimensions are relatively large, resulting in easy human recognition and manipulation.
- It has a high information storage density.
- Machine-readability is being improved through simpler character recognition methods, special fonts, magnetic "stripes", etc.
- Scanning enables "machine reading" of graphic information.
- Since the information on paper cannot readily be changed without leaving a trace, it has excellent documentation qualities.

He says that:

> "Enhanced by the law, a bad cheque, for example, is a criminal offence, a basis for prosecution and as such difficult to replace by an 'electronic document'."

On the other hand, it could be argued that cheque forgeries are easier to carry out with paper than with fraudulent manipulation of financial information inside a computer system. As data security procedures improve, it will require highly intelligent thieves to penetrate computer systems.

Stiefel concludes with the belief that:

> "An electronic pulse will do everything to execute a transaction, but it will not replace the cheque in the authorization of the transfer of property itself."

Another inhibiting force in the development of new bank automation systems is the fact that the public must be educated in the ways of electronic money. Many people have come to believe in the convenience and record-keeping value of cheques. Others avoid or misuse bank services. Some keep their money in mattresses and pay all their bills in cash. Some are afraid of loans and charge accounts.

Because of bad debts and frauds, an automatic payment and loan network will require built-in protection that is both automatic and foolproof. The problem of verifying a cardholder's identity poses a major technological challenge to the "chequeless" society. Another key security topic is personal credit ratings. These too will have to be computerized for quick and automatic access. This could be a serious problem.

"The safe extension of credit until now has been limited by by ability to get accurate performance data", says Dr. Harry C. Jordan, president of Credit Data. "The credit bureau industry has not kept pace with automation [67]."

A nation-wide bookkeeping network will require a standardized financial identification card and numbering system. In Canada the Social Insurance Number might prove adaptable. But first, the banking industry and its credit card competitors must sit down and agree on some standardization.

Another inhibiting force could be the shortage of human resources to develop and implement the new systems. As Zipf has stated [68]:

> "Our progress in the evolution of the chequeless cashless society will be conditioned not so much by equipment resources as by human resources. Considering the almost incredible technological advances which have been and are being made by equipment manufacturers, I am convinced that our continuing supply of equipment is relatively assured. Even now, as our second generation equipment is giving way to a third, there is undoubtedly a fourth on the ramp and a fifth being readied in the hangar.

> But who will pilot this increasingly sophisticated gear? Who will understand its fantastic speed and capability? Clearly our supply of human resources is more limited and more critical."

In today's payment system, the consumer has many options. He can pay cash, write a cheque, obtain a loan, etc. A future "chequeless" system must permit all these options to continue and perhaps offer new options. But a massive educational campaign is likely to be required before the public accepts it fully.

In a recent study, John Diebold predicted that in future about two thirds of the payments by cheques would be automated, but one third would never be automated. In other words, one third of the cheques would remain in use.

Moreover, it is probable that cash will endure for a number of reasons. For example, there will always be street vendors who cannot operate with charge cards and bank accounts. In addition, people will pay cash for small items for the same reason they do not write cheques to buy chewing gum. Bank service charges would double the price.

An inhibiting factor to the provision of computer services by banks is the complexity of the legal problems they might encounter. As Fenwick [69] has pointed out, the cost of litigating computer cases will dwarf the cost of an anti-trust case. He states that some of the considerations having legal signifinance in providing EDP services are location and security of the computer operation, scope of the service to be provided, pricing of service, confidentiality of programs and data to be used, documentation of customers' needs, impact of special credit or statutes, and the contract under which service is to be provided.

Another inhibiting factor to the advent of the "chequeless" society is the inherent conservatism of people in the banking industry. Bankers have traditionally emphasized their lending functions — not their paperwork systems. In a survey of U.S. bankers, Reistad [70] found that less than half of them expected the arrival of a chequeless society.

On the other hand, there will be forces at work to accelerate the implementation of banking automation. One of these forces will be economic. Electronic banking systems can produce significant reductions in operating costs. On the chequeless society's potential savings to the cheque users and processors, John J. Clarke, vice-president and special legal counsel for the Federal Reserve Bank of New York, has written [71]:

> "Preliminary indications are that if a direct funds transfer (DFT) system is in widespread operation by 1975, the average cost per transaction will be 7-1/2 cents with a spread of from 3 cents to 12 cents in individual transactions. Present costs of the demand deposit or chequing account system appear to run to about 13 cents per transaction to which must be added another 12 cents per transaction if the transaction involves an extension of credit. If these figures are even nearly right and I believe they are, use of the DFT system could at best save 17-1/2 cents per transaction on average and at worst save 5-1/2 cents per transaction on average."

Another force is that, as one bank embarks on an ambitious automation program, other banks may feel forced to follow the leader. The American Bankers Association believes that in today's industry the individual bank, no matter how large or important it may be, is having less and less to say about its own destiny and is becoming conversely more and more dependent on the direction of the banking industry itself [72].

O'Brien [73] has suggested that the financial information utilities of the cashless chequeless society would require only the extension of many of the present operations of existing banks. He points out that many banks already have computerized their demand deposit and savings deposit accounting. Some banks are offering preauthorized bank loans and preauthorized automatic charges to accounts or transfer of customer funds. Many banks and corporations currently provide for the direct deposit of payroll funds to employees' chequing accounts.

It is difficult to predict whether the optimists or pessimists are right with regard to the future chequeless cashless society. Kramer has predicted that within five years the chequeless society will be upon us [74]. The American Bankers Association has predicted that 86% of the bills an average person now pays by cheque may be paid by electronic transfer by 1977 [75]. It is reasonably certain, however, that during the next ten years, some parts of the new systems described above will be implemented in the Canadian banking industry.

IV. POTENTIAL FUTURE PROBLEMS

If some or all of the systems described in the preceding chapter are developed — and it is certain that some will be — the following are some potential problem areas which may develop.

As banks expand their computer systems and develop on-line systems with remote-access terminals, the problems associated with providing adequate data security will become more acute. As time-sharing methods of computer use increase, data security problems also increase. In sharp contrast to the old batch processing method of computer utilization under which programming jobs were run sequentially, often leaving the heart of the computer idle while data is being read in and results are being written out, time-sharing allows nearly full utilization of the computer's capacity by enabling more than one user to use the computer at once. Each user has his own input and output terminal connected to the computer and by means of a complex master program the computer is able to switch its attention among the commands of the various users virtually instantaneously, giving the impression to each of the users that he alone is using the machine.

Thus, some users may be reading data in and others printing results, while still others are having their programs executed by the computer's central processor. Under such a time-sharing arrangement, the computer is used more efficiently and economically than it is under the old batch processing arrangement. The net result is that each user is given a functional equivalent of his own computer at a fraction of the price that a computer of his own would cost him. However, under a time-sharing arrangement there occurs the simultaneous exposure of several distinct bodies of data in the machine, creating the risk that one user might gain access to the data files of another user, thus compromising the privacy of the other user and of a third party's whose personal data is being stored or processed in the time-sharing system.

Even if the time-sharing system employs careful data security precautions such as access codes, it is still possible to break the access code and gain the unauthorized information. At Massachusetts Institute of Technology, the home of time-sharing, students were able to break elaborate codes that were supposed to protect the privacy of the users of its Project MAC computers. In one instance, the students even tapped into lines carrying transmissions from the Strategic Air Command in Omaha [76].

A computer expert can penetrate time-sharing systems. Professor E.L. Glaser of Case Western Reserve University in Cleveland is such a skilled penetrator. After learning the standard operating procedures for the system and then thinking about it for a few hours, he has been able to break into a system after five minutes at a terminal.

In one system that Professor Glaser tested, the security system was considered to be good but he discovered one "trapdoor" in a relatively short time. He wrote a simple program which went through every file in the system, found the owners' names and passwords, extracted all passwords and stored them in a new file after scrambling them so they could not be recognized. He was then able to read any file at any later time.

In another case, Professor Glaser tested the security measures of a new commercial time-sharing system. The security measures were again considered to be good, but again he found a number of "trapdoors". Within five minutes at a remote terminal he was able to "crash" the whole system, bringing it to a complete halt [77].

The extensive computer communications network of Metropolitan Life Insurance Co. has recently been the victim of sabotage, allegedly by union members striking against the company's computer vendor, Honeywell [78]. By telephoning a tape recording of the signals used by a central computer to poll remote data stations, the saboteurs managed to prevent the printing of processed data in some 25 local Metropolitan Life offices.

Canning [79] has suggested that for the vast majority of time-sharing systems in use today, it is unwise to put any highly sensitive data on-line to the computer because the data security procedures are not adequate. He believes that in order to put sensitive data in on-line computer files, it is necessary to:

1. limit the number and types of users that would use the system;
2. limit the number and types of terminals and location of those terminals;
3. limit the sensitivity of the data in the files as much as possible so as to limit the potential threats;
4. design and build clean software, particularly the operating system, and incorporate security features in the design.

Carroll [80] has discussed the problem of providing adequate data security for time-shared systems. He concludes that:

> "The security of existing resource-sharing systems is not good and there is a risk of exposure or loss of sensitive information. Adequate protection of information is possible within the state-of-the-art but this would be costly, especially in terms of requirements for specialist personnel. Most security provisions when implemented would tend to reduce operating efficiency and flexibility."

Van Tassel [81] has suggested that:

> "No security system can approach a zero risk of loss. Security is based on a cost-benefit concept. That is,

> that it would cost more to violate the confidence of the centre than would be gained from such violations. There is some satisfaction in the fact that a small amount of protection usually means that a large cost (in effort, money, danger, etc.) will be needed to violate the security of the centre."

The author is aware of some significant efforts being expended by several of the larger Canadian chartered banks to improve their data security systems and techniques. Despite the difficulty of achieving perfect data security, it is reasonable to expect that the Canadian chartered banks will achieve security that is good enough to preserve confidentiality and prevent computer fraud. The banks will need to achieve this kind of security because, with time-shared systems, any bank teller will be able to have access to a computer terminal and thereby to some central computer files. Moreover, the bank will need to ensure that its communication circuits cannot be penetrated by outsiders and if they are penetrated that no sensitive information can be stolen.

Another problem related to data security is that of identifying whether a card is valid or not. If everyone carrys a credit card in the chequeless society, how will the storekeeper know whether the card is counterfeit? How will he know the customer did not steal the card or find it in a gutter? Ultimately, the banking industry may have to settle for a system that is less than 100% effective and write off the losses on the remainder as a cost of doing business.

Photographs can be embedded in the cards to make them tamperproof, but then a sales clerk, prone to error and perhaps bribes, would have to make the identity check and, of course, there is the possibility of plastic surgery.

Some people have advocated the use of "voiceprints" — electronic "pictures" of an individual's voice — to identify cardholders. Conceived in 1941 as a way for the deaf to "read" speech, the voiceprint machine analyzes patterns of pitch and volume and transcribes each variation into a picture. One of the chief developers, Physicist Lawrence Kersta, claims that everyone's voiceprint is as unique as his fingerprints, and that any skilled technician can identify a voiceprint with more than 99% accuracy. Other scientists have disputed his claims [82].

Nonetheless, a crime in St. Paul, Minnesota, was solved through the use of voiceprints [83]. Around midnight on May 22, 1970, St. Paul police got an anonymous call asking help for a woman about to give birth. Two policemen sped to the scene but found a darkened house. While one policeman went round to a back door, a sniper suddenly opened fire from across the street. The second policeman fell mortally wounded.

It seemed a random attack on "police in general", and the only clue was the telphone call, which had been routinely taped. To find a matching voice, policy interrogated 13 women in the neighbourhood. At each interview they made voiceprints. Because her voiceprint matched the taped call, a woman was arrested and later indicted for first degree murder.

It is possible that a new type of credit card, similar to one recently described by Johnson [84], might provide an effective solution to the identification problem. This card works on the principle that it has a cash balance written on the card in magnetic code and each time a purchase is made the card is put in a terminal to have the appropriate sum deducted automatically. This card uses a new way of recording the vital code number identifying the card — an essential check against theft or forgery. Instead of using a strip of magnetic material, this card has a double row of minute radio aerials laminated into it. Each aerial is tuned to oscillate at a specific radio frequency, which is coded to represent a number from zero to nine. This gives the card a permanent identifier which can be read by the terminal. Changeable figures, such as the cash balance on the card, are recorded in a magnetic stripe in a more conventional way.

Regardless of the type of security system that is eventually adopted, computer utilities may face the threat of underworld infiltration [85].

Related to the problems described above of providing adequate data security, is the possibility that computer fraud may become more difficult to prevent as computer systems become more complex. On the other hand, it could be argued that with more complex computer systems, a thief will need to be more intelligent in order to commit computer fraud successfully. Stiefel [86] has stated that:

> "In banking it has become increasingly common to use one large central facility and to connect the branches with data communications. When money is deposited in a branch office, for example, this fact is sent to the central computer through telephone facilities, cables and exchanges. This offers then an excellent opportunity to rob a bank without ever setting foot in it — probably considered a vast improvement over the existing methods of hold-ups.
>
> However, an equally likely opportunity for electronic fraud lies in the operation of the computer room itself. As data processing becomes an increasingly routine operation and less skilled and probably lower paid workers will be employed, the incentive for fraud is bound to increase."

As banks develop more elaborate computer systems using remote-access terminals, they will gain the ability to track the movements of the credit-card holder even more rapidly and more precisely than today's systems can. Scaletta [87] has suggested that:

> "We may be quite near to a cashless chequeless society in which all of our financial transactions would be taken care of by a credit card which would be inserted

> in a remote computer terminal to register each transaction. The telephone companies could use their systems, which in essence are computers, to keep track of all calls we make. The postal department could use optical scanners to compile data on persons with whom we correspond. Some of the airline reservation systems are already maintaining passenger lists for two to three months after each flight so that these lists may be accessed by investigators who are checking on the travels of certain individuals."

If we add the possibility that future banking systems will be able to keep track of all purchases made by a cardholder, it is possible that the average citizen could find himself under the scrutiny of a very powerful computerized tracking system.

Even if we do not achieve a complete chequeless cashless society in the near future, it is reasonably certain that there will be a significant increase in the importance of banks in our society. Banks are likely to have an increasing influence in the entire credit area. It is possible that in the future, credit decisions will be made by computer systems on the basis of the current status of a customer's account and his past performance as recorded on magnetic tapes in the bank's computer centre. If this should materialize then it will be very important that the records be accurate, and that the people who handle the records have good integrity, because this could affect an individual's purchasing power in profound ways.

If banks should place greater reliance on computers in the future, then there will be an increased tendency for information to be unquestioned as it emerges from computer systems. Thus, information could be wrong and still be regarded as accurate by readers. Computers tend to add credibility to inaccurate data. This could prove to be a serious problem if banks rent terminals to retail stores and clerks feed incorrect data into the banks' computers. A similar problem could also occur with manual systems, but the fact that computers add credibility to inaccurate data makes it necessary to take additional precautions to ensure the accuracy of data fed to computers.

An important victim of an electronic fund transfer system would be banking's float — the millions of dollars in transit among banks on any given day. Many people play the float regularly by writing cheques for money that is not in their account and covering the overdraft two or three days later. In effect, this creates an interest-free loan. Many merchants and small businesses survive on this. Corporations use the time lag in the pipeline too, but in more elaborate ways. For example, a cash manager with accounts around the country might switch balances by depositing out-of-town cheques, thereby increasing his money supply while the cheques navigate the pipeline and then invest the funds over the weekend or even overnight. If the bank float does disappear in future, the Canadian chartered banks may have to make special credit provisions for their customers to prevent the loss of convenience provided by the float.

It is possible that, as each of the Canadian chartered banks develops an on-line computer system involving a computer communication network to connect all its branches to a large-scale central computer, some of the banks may consider merging with other banks in order to avoid duplication of the communication facilities. However, it should be recognized that the cost of the communication facilities for a large on-line banking system would be only a fraction of the total cost of the system. Moreover, it could be argued that today, some city street intersections have four different banks — one on each corner — and this could be regaraea as a wasteful duplication of effort. The fact that people differentiate among banks today, even though most of the banks offer similar services and facilities, could be a good argument to indicate that mergers will not occur in the future. However, if mergers do occur, the resulting reduction in competition could create problems.

V. CONCLUSIONS

The banking industry is different from other industries for at least two reasons. First, it can get large amounts of money more cheaply than anyone else. It therefore exercises a significant influence over every other industry in the country. Secondly, banking has access to large amounts of important information about individuals, companies and communities.

Over the years, banks have proven themselves to be responsible organizations. Banks have also stuck to banking because as an article in "Business Week" has suggested [88]:

> "The banks have a long standing conviction that to own industries or to lead nations is to flirt blindly with that capricious wench, Dame Fortune: Kings and economies may rise and fall but the lender and his spread presumably go on forever."

It is reasonable to expect that a change to a cashless chequeless society will come about on a gradual basis and will involve an orderly evolution to a system of less cash and fewer cheques. How far the system develops or what exact form it takes will probably be limited only by the extent of public acceptance and the rate of integration of the various types of systems involved.

It is likely that in the future, as the banks develop more advanced large-scale computer systems, they will become even more influential in industry and commerce. Not only will they have an opportunity to penetrate the credit bureau business, but they will also be able to penetrate the computer service bureau business and perhaps even become computer utilities. As a result the banks will possess, control, or have access to an ever-widening pool of information about individuals and corporations. The responsibility thus placed upon the banks — for safeguarding privacy and security — will be correspondingly increased.

Many of the Canadian chartered banks are devoting considerable attention, time, effort and money to improve the data security systems associated with their computers, particularly those with remote-access terminals. As the banks develop more elaborate computer systems, they will need to continue to devote this effort to solve the new, more complex security problems that may arise.

It is conceivable that despite their best efforts, banks will not be able to provide adequate data security without fragmenting some of their computer files in order to make computer fraud and disclosure of confidential information more difficult. Such fragmentation of computer files might reduce the utility of those files but it may be a necessary step to take. However, it is reasonable to expect that in due course, adequate data security techniques will be developed to make it possible for the banks to have secure systems without the need to fragment their files.

If the banks move to expand their services as a result of more powerful computer systems, they may collide with other groups, such as the insurance industry, accountants, investment bankers, mutual funds, loan companies, credit bureaus, retailers and service bureaus.

The banks in Canada have established good reputations for preserving confidentiality and protecting privacy. Any additional safeguards will cost money, with the expenses involved borne ultimately by the public at large. Hence any regulations to increase the degree of protection of privacy must take full account of the costs involved and the specific benefits to be gained. Such regulations should be directed at those areas where problems can be clearly identified and should not be aimed at intangible goals.

REFERENCES

[1] Fitzakerley, V.F.: "The Revolution in Banking". Canadian Chartered Accountant, January, 1970, p36.

[2] Toronto Daily Star, December 4, 1971, p8.

[3] Interview with Adams, A.S., Member of The Canadian Computer-Communications Task Force.

[4] See Reference [1].

[5] See Reference [3].

[6] See Reference [3].

[7] Powledge, F.: "Learning to Live with the Credit Card". Esquire, September, 1971.

[8] Financial Post, December 11, 1971, p38.

[9] See Reference [7].

[10] "Money Goes Electronic in the 1970's". Business Week, January 13, 1968.

[11] See Reference [3].

[12] See Reference [10]

[13] Martin, J. and Norman, A.R.D.: The Computerized Society. Prentice-Hall, 1970, p82.

[14] White, G.C. Jr.: "Installation of a GIRO Payment System in the United States". Datamation, November, 1969, p195.

[15] Graddy, J.W.: "The National GIRO". The Computer Journal, October, 1967.

[16] See Reference [13], p86.

[17] See Reference [14].

[18] Kramer, R.L. and Livingston, W.P.: "Cashing in on the Checkless Society". Harvard Business Review, September/ October, 1967, p149.

[19] See Reference [10].

[20] See Reference [3].

[21] See Reference [3].

[22] See Reference [3].

[23] McDougall, R.A.: "Panel Discussion on Computers, Communications and Canada". Canadian Computer Conference, Toronto, September 17, 1971.

[24] See Reference [3].

[25] Ross, I.: "The Credit Card's Painful Coming-of-Age". Fortune, October, 1971, p108.

[26] Hanlon, J.: Computerworld, September, 1971.

[27] Computerworld, December 15, 1971, p3.

[28] Nader, R.: "Computers and the Consumer". Computers and Automation, October, 1970, p21.

[29] Boeth, R.: "The Assault on Privacy". Newsweek, July 27, 1970, p19.

[30] Aitken, J.: "Privacy Takes a Beating in Credit Buying". Toronto Telegram, April 7, 1971.

[31] Hanlon, J.: "Consumers Get Some Protection With Credit Law". Computerworld, April 28, 1971, p1.

[32] See Reference [25], p156.

[33] Toronto Globe and Mail, April 23, 1971.

[34] Ziegel, J.S.: "The Fourteen Flaws in Ontario's Credit Bureau Legislation". Toronto Daily Star, May 17, 1971, p8.

[35] Warner, M. and Stone, M.: The Data Bank Society. George Allen & Unwin Ltd., 1970, p146.

[36] Jacobson, R.V.: "Providing Data Security". Automation, June, 1970, p90.

[37] See Reference [25], p111.

[38] See Reference [7].

[39] See Reference [7].

[40] Henderson, R.P.: "Record-Keeping in the Space Age". Vital Speeches of the Day, August, 1970, p507.

[41] Westin, A.F.: Privacy and Freedom, Atheneum, 1967, p165.

[42] Rogers, J.G.: "Who Needs Money?". Parade, December 26, 1971, p6.

[43] Allen, B.R.: "Computer Fraud". Financial Executive, May, 1971, p38.

[44] See Reference [43], p39.

[45] Wasserman, J.J.: "Plugging the Leaks in Computer Security". Harvard Business Review, September/October, 1969, p124.

[46] Allen, B.: "Danger Ahead! Safeguard your Computer". Harvard Business Review, November/December, 1968, p99.

[47] Toronto Daily Star, December, 4, 1971, pl.

[48] Financial Post, December 4, 1971, p3.

[49] Osvald, T.: "Feasibility Study of a Cashless Society in Sweden". (SIBOL) Project, O.E.C.D. Report, April, 1971, p18.

[50] See Reference [18], p142.

[51] See Reference [49], p4.

[52] See Reference [42], pp6,7.

[53] See Referenee [18], p143.

[54] See Reference [7].

[55] Reistad, D.: "Credit Cards - Stepping Stones to the Chequeless Society?". Computers and Automation, January, 1967, p26.

[56] See Reference [25].

[57] See Reference [25].

[58] Toronto Globe and Mail, September 30, 1971, pB9.

[59] Robertson, J.: "Paying by Computer". New Scientist and Science Journal, September 17, 1970.

[60] "Computers and Banking", Commercial Letter, Canadian Imperial Bank of Commerce, April, 1969, p4.

[61] See Reference [10].

[62] See Reference [10].

[63] Miller, A.R.: The Assault on Privacy. The University of Michigan Press, 1971, p75.

[64] See Reference [63], p79.

[65] Toronto Telegram, April 6, 1971.

[66] Stiefel, R.C.: "A 'Checkless' Society or an 'Unchecked' Society?" Computers and Automation, October, 1970, p32.

[67] See Reference [10].

[68] Zipf, A.R.: "The Computer's Role in the Dividends or Disaster Equation". Computers and Management, The Leatherbee Lectures, Harvard University Graduate School of Business Administration, 1967, p73.

[69] Fenwick, W.A.: "Marketing EDP Services - Reviewing the Legal Considerations". Computers and Automation, November, 1971, p8.

[70] See Reference [55].

[71] Clarke, J.J.: "Checkout Time for Checks". The Business Lawyer, July, 1966, p93.

[72] American Bankers Association Conference Report. Datamation, August, 1968, p72.

[73] O'Brien, J.A.: "The Bank of Tomorrow: Today". Computers and Automation, May 1968, p27.

[74] See Reference [18].

[75] See Reference [73].

[76] Scaletta, P.J.: "The Computer as a Threat to Individual Privacy". Data Management, January, 1971, p22.

[77] EDP Analyzer, May, 1970, p2.

[78] Computerworld, December 15, 1971, p1.

[79] See Reference [77], p12.

[80] Carroll, J.M. and McLellan, P.M.: "The Data Security Environment of Canadian Resource-Sharing Systems". Management Science, December, 1970, p66.

[81] Van Tassel, D.: "Information Security in a Computer Environment". Computers and Automation, July, 1969, p28.

[82] "Task Force Report: Science and Technology", a report to the President's Commission on Law Enforcement and Administration of Justice, prepared by the Institute of Defence Analysis, U.S. Government Printing Office, Washington, D.C., 1967, pp218, 222.

[83] Time, January 10, 1972, p45.

[84] Johnson, T.: "Science and the Paymasters". New Scientist and Science Journal, September 30, 1971, p741.

[85] See Reference [10].

[86] See Reference [66], p34.

[87] See Reference [76], p23.

[88] See Reference [10].

STUDIES COMMISSIONED BY THE TASK FORCE

The Nature of Privacy - D.N. Weisstub and C.C. Gotlieb.

Personal Records: Procedures, Practices, and Problems - J.M. Carroll and J. Baudot, Carol Kirsh, J.I. Williams.

Electronic Banking Systems and Their Effects on Privacy - H.S. Gellman.

Technological Review of Computer/Communications.[1]

Systems Capacity for Data Security - C.C. Gotlieb and J.N.P. Hume.

Statistical Data Banks and Their Effects on Privacy - H.S. Gellman.

Legal Protection of Privacy - J.S. Williams.

Vie Privée et Ordinateur Dans le Droit de la Province du Québec - J. Boucher.

Regulation of Federal Data Banks - K. Katz.

Regulatory Models - J.M. Sharp.

Ordinateur et Vie Privée: Techniques et Contrôle - C. Fabien.

The Theory and Practice of Self-Regulation - S.J. Usprich.

Privacy, Computer Data Banks, Communications and the Constitution - F.J.E. Jordan.

International Factors - C. Dalfen.

[1] A joint Study by the Privacy and Computers Task Force and the Canadian Computer/Communications Task Force, to be published by the latter.