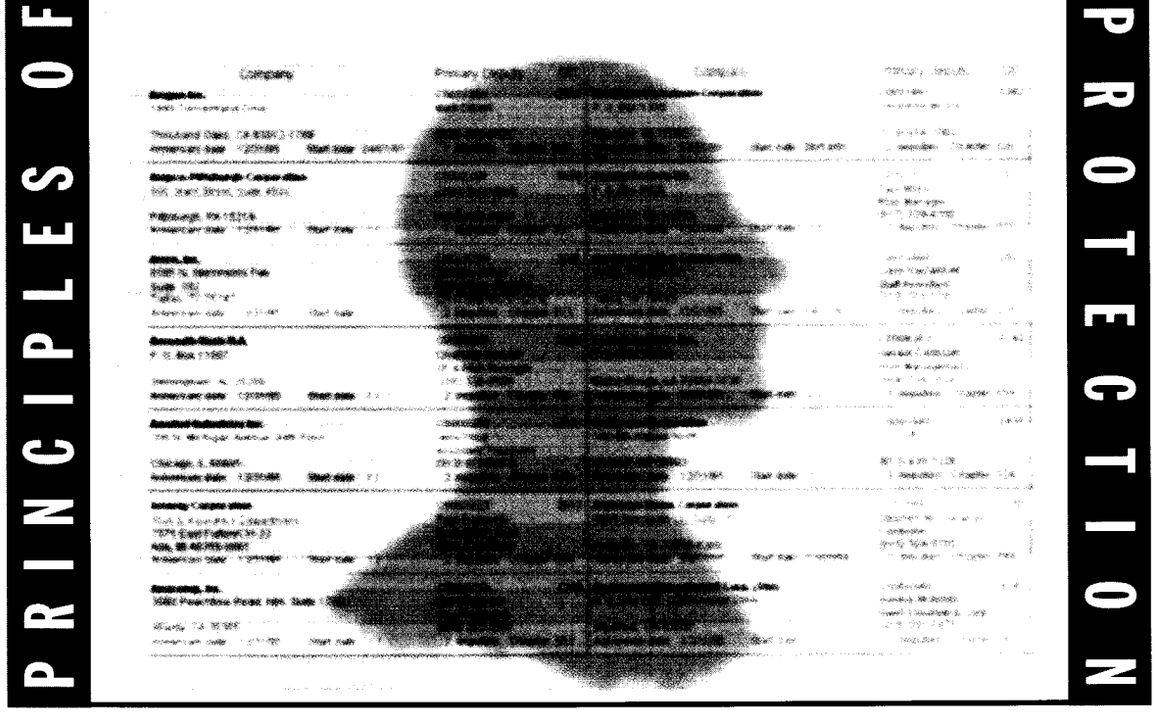
PRINCIPLES OF PERSONAL DATA PROTECTION



by Pierrôt Péladeau

In the spring of 1988, a financial institution installed a new noncompensated funds management (NFM) system designed to provide its 5.5 million customers with instant access to their money, thus ending the three- to five-day freezing of interbranch and automatic teller check deposits. But within hours, the institution was deluged by protests from customers. Contrary to the designers' expectation, many of the checks customers attempted to cash had been frozen by the bank's computers.

Unfortunately, the NFM banking system had been designed to serve very basic transactions by individual customers with all of their accounts and loans in the same branch. The further that actual customers' situations departed from this profile, the more likely the NFM system would produce erratic decisions. Many businesses were not able to pay their employees or providers. Many furious customers closed their accounts and switched to competing banks. Others complained of discrimination or privacy invasion. Consumer organizations brought the problem to media attention. Meanwhile some unscrupulous customers wrote bad checks that were approved by the malfunctioning computer. After only a few days of operation, the NFM system was disconnected. When system administrators were unable to correct the problems, six years of design work was scrapped.

As organizations grow increasingly dependent on electronic information systems, the more likely it becomes that faulty design or operation can create significant and costly problems.

The disastrous fate of the NFM system is a perfect example of the kind of risks involved in the development and operation of computerized information systems. Dealing with design errors or implementation difficulties has become almost a standard procedure when installing or updating these systems. Unfortunately, many designers and managers do not recognize that information management systems often make decisions automatically about individual customers.

Pierrôt Péladeau is vice president-research and development at Progesta Inc., an information management consultant firm in Montreal.

As organizations and people grow increasingly dependent upon computers, the more likely it becomes that faulty system design and operation can have significant and very costly effects.

System designers and organizational managers must cooperate to anticipate the potential problems and reactions before installing or modifying information systems. Such assessment should consider the administrative, legal, social, ethical and public relations issues that are likely to arise.

SYSTEM IMPLEMENTATION

Today's information systems involve thousands of lines of programming instructions as well as intricate interactions between numerous pieces of computer and communication hardware. System users have to undergo training to learn proper operation. Often, entire departments, functions or organizations are meant to be changed by the introduction of a new system. Given the complexity of the undertaking, problems such as bugs, inadequacies, user errors or resistance are bound to occur.

Even so, many personal information systems are rushed into operation without any kind of on-site testing to detect problems. Often, there is insufficient supervision of system implementation or user training. Moreover, there is usually little communication to the system's data subjects, who could be valuable partners by providing information about overlooked design issues or doubtful system behavior.

The most common information management problem is collecting and retaining too much information. Despite the fact that some data has limited value in making decisions, it is often retained—in too many copies and for too long—usually because a system has the capability to collect and store it.

For one public utility, the time required to read outdated customer information added up to thousands of hours every year. The outdated information increased the time already wasted by producing 40,000 customer service notes every month (of which fewer than 3 percent were later deemed to be "somewhat pertinent" in service delivery). The problem becomes quite evident the moment a price tag is put on this kind of mismanagement.

It is a demanding task for organizations to define what personal information is truly important to carrying out a given activity, and the challenge of keeping data current and accurate is perpetual. To assist organizations, a number of guidelines called "principles of personal data protection" have been developed. In addition to their use in privacy protection, these standards can help organizations reduce operating risks while improving information management.

The "quality of personal information" principle calls for organizations to make sure the information they are using and storing meets the level of quality necessary to support business decisions. Observing this principle's requirements is one of the most significant risk-diminishing factors because most problems result from using inappropriate, inaccurate or outdated information.

The "security" principle ensures the organization's control over its data and prevents incidents that could trigger a confidence crisis with an organization's customers. A security breach is a major operational and liability exposure for any organization.

Too often, organizations with sound security policies that cover daily system operation become negligent when disposing of unneeded or outdated material. Organizations may sell obsolete equipment without removing valuable information from the hard drives. It is common to donate paper that has been used on one side to schools or daycare centers for use as drawing material. Customer records from health insurance, public utility and transport companies have taken this destination. In 1994, the media were alerted when a list of 90,000 telephone calling card numbers ended up in a school. In addition to the inconvenience of canceling the cards, the phone company spent nearly $500,000 to issue replacements. Security and proper information management should apply to the entire life cycle of the data, not only when it resides within a computer system.

The "individual participation" principle (giving the data subjects the right to access, review and correct information) also contributes to the quality of information and thus to the quality of decisions. Openness is important. Explaining how (and why) information will be used, collected and stored can improve the data subjects' confidence and the organization's reputation. Customers will generally be more cooperative in supplying accurate information about themselves if they believe the information will be kept confidential and used for legitimate purposes such as improving service or safety. Without such

A PERSONAL DATA PROTECTION CHECKLIST

In September 1995, the Canadian Standard Association's Technical Committee on Privacy unanimously adopted the Q-830 standard setting a model code for the protection of personal information. This 11-page standard is organized around 10 interrelated principles:

1. **Accountability**
2. **Identifying Purposes**
3. **Data Subject Consent**
4. **Limiting Collection**
5. **Limiting Use, Disclosure and Retention**
6. **Accuracy**
7. **Safeguards**
8. **Openness**
9. **Individual Access**
10. **Challenging Compliance**

CSA is studying the possibility to transform this standard into audit criteria for a certification program similar to those existing under the ISO 9000 series for quality management. Meanwhile, Q-830 can already be used as a basic personal data protection checklist by system designers.

assurances, they may assume information about them will be sold or otherwise misused. Many customers will be reluctant to share personal information, and in extreme instances, they may provide false data. The expected operating advantages gained from the information system can be transformed into liabilities if an organization's computers unwittingly process false data.

The "purpose definition" principle helps in ensuring the quality of decisions by reminding organizations that personal information collected for a specific reason might have a very different meaning or value when used for a different purpose. In one instance, it was found that prescription drug information that was sufficiently accurate for billing purposes presented high error rates if it was used to make medical decisions. The error rates of the combined drug/dose/days data was around 21 percent. Although it may appear tempting to apply existing data for new purposes, it is also easy to see the potential problems of using data in a context for which it is unsuited. Even if the risks are less hazardous than the prescription drug example, potential problems related to this sort of information misuse are bound to plague organizations that do not consciously strive to avoid them.

IMPACT ASSESSMENT

Good implementation and information management procedures are not sufficient by themselves to correctly cope with the risks involved with developing and operating information systems. How the users and data subjects will react to the system is a central question that must be addressed. An information system is a complicated tool, often operating in a complex social environment in which the users and data subjects are interacting with each other and the equipment. This interaction can produce unanticipated consequences or trigger reactions that may endanger the system itself.

Predicting how everyone affected by an information system is likely to interact must be part of a comprehensive impact assessment. Improper anticipation of how customers will use an organization's products and services (as was the case with the banking example discussed earlier) will likely invalidate many of the assumptions made during the system design. Poor information can lead to poor decisions. Similarly, if organizations solicit the opinions of the employees who will use the system, they can prevent many potential problems. For instance, it is important to ensure that restructured work processes (often designed as much to accommodate the information system's requirements as those of the users) actually are more efficient than the processes they are replacing. Even if the new process is more effective, employee resistance to the new way of doing things may dilute some of the advantages.

There is a large number of documented instances of boycotts and sabotage attempts against new information systems in the fields of health and social services (agencies that typically process very sensitive personal information). In many cases, disruptions occurred because professionals felt that the system was transforming their role from service provider to one of information collector or system operator. This was clearly the case for one hospital's emergency department physicians who threatened to resign en masse to protest the fact that they were wasting more time responding to information requests than to the needs of their patients.

As new organizational data infrastructures develop and transactions in which individuals participate become more automated, understanding the risks of operating information systems becomes crucial. The consequences of faulty design or poor implementation will affect larger numbers of people and organizations. In this context, preventive measures are much less costly than the risk of damages resulting from system failures. Sound implementation procedures, good management and appropriate system impact assessments are key sets of measures for dealing with information effectively. RM

STEPS FOR DEVELOPMENT OF INFORMATION SYSTEMS

1. Assess the organization's environment: Evaluate the needs, demands and concerns of users and customers. Assess the external environment (laws, standards, customs).
2. Evaluate the proposed system: What is the nature of the transaction? How sensitive is the information? Can it be misused? How do individual data subjects differ? How will they interact with the system?
3. Evaluate the risks that could result from poor information management or system failure. What are the business interruption or operating risks? Is there a potential for adverse publicity?
4. Apply personal data protection principles.
5. Apply proper system security. Ensure outdated equipment or printouts will be disposed of properly.
6. Pilot test the system.
7. Train and supervise the system users.
8. Inform customers how data will be used and stored.
9. Implement feedback and adjustment mechanisms.