



*Prescient*

# Ensuring Privacy of Information Encrypted Relational Database Model (ERDM)

A Solution WhitePaper by Prescient International Inc.  
January 2002

Delivering the Future . . . Prescient Solutions.

[www.prescient.net](http://www.prescient.net)



**Prescient International Inc.**

4950 Yonge St, Suite 600  
North York, Ontario, Canada  
M2N 6K1  
(416) 221-3200

***Ensuring Privacy of Information  
Encrypted Relational Database Model  
(ERDM)***

***Table of Contents***

1. Executive Summary .....	1
2. Background .....	2
3. Issues with Lack of Privacy .....	3
4. What is Privacy? .....	4
5. Difference Between Security, Privacy and Confidentiality ....	6
6. Privacy Enhancing Technology - What is it .....	7
7. Description of ERDM .....	7
8. Benefits of ERDM .....	9
9. Prescient Background.....	9
10. Case Use - ERDM in Electronic Health records .....	10
11. Conclusion .....	11

*Copyright 2002 Prescient International Inc. All rights reserved.*

*Information in this document is subject to change. This document contains information proprietary to PRESCIENT INTERNATIONAL INC. (Prescient). Transmittal, receipt, or possession of this document does not express license, or imply rights to use, sell, design, manufacture, or have manufactured from this information. No reproduction, publication, or disclosure of this information, in whole or in part, electronic or otherwise, shall be made without the prior written authorization from an officer of Prescient. Prescient International may have pending trademarks, or copyrights or other intellectual property rights covering subject matter in this document.*



***Delivering the Future . . . Prescient Solutions.  
[www.prescient.net](http://www.prescient.net)***



## 1. Executive Summary

Privacy is the most important issue for any developing e-business venture. The ability of an organization to securely store information relating to its employees, its client base, or anybody that does business with it is a crucial element in building trust. Without the trust of clients, end users, or even internal employees, the information that is collected and stored in electronic format can be as much a weapon as a tool against both individuals and businesses.

Database and Knowledge management in 2002 is not just an issue of data transmission and security protocols. It is not enough for an organization to simply lock out intruders, especially when the organization is connected to the Internet, or carries out its business in an electronic format. In the growing world of electronic transmissions, the need to rely on the Fair Information Practices such as the CSA Model Code for the Protection of Personal Information is becoming a greater and more integral part of doing business.

In order to protect its ability to ensure future business and revenue, it is imperative that Privacy, Security and Confidentiality be viewed as tools, as much as workflow metrics, sales and customer care are now part of everyday business life.

The federal Privacy Commissioner, George Radwanski, recently said in a speech, "build privacy into the system, as an essential component. Technology, science, and information management should serve our values, and be determined by them—not the other way around. Privacy should determine the architecture of the system."<sup>i</sup>

The point the Commissioner raises in this quote is that Privacy, Security and Confidentiality are each key elements to a successful protection of an organization's ability to do business.

If e-commerce is ever to take off, consumers must feel comfortable with their ability to carry out a transaction, without the threat of having their personal, private and confidential information stolen or even at a perceptible risk.

For example, EKOS Research Associates recently found that only 22 percent of Canadians would be comfortable giving their credit card number on line. That figure rises to 33 percent of confirmed Internet users, but falls to 11 percent for casual Internet users<sup>ii</sup>. According to a recent Statistics Canada report, in 2000, Canadian businesses had received \$7.2 billion in customer orders over the Internet in 2000, up 73.4% from \$4.2 billion in 1999. In 1999, 10% of businesses reported selling goods and services on line. In 2000, however, that number fell



***Delivering the Future . . . Prescient Solutions.***  
***[www.prescient.net](http://www.prescient.net)***



dramatically to only 6% of businesses. These 6% of businesses selling on-line accounted for one-quarter of all gross business income<sup>iii</sup>.

What's more, 31% of business enterprises with more than 500 employees sold goods or services over the Internet<sup>iv</sup>, meaning that large amounts of information are being used in order to conduct business transactions. This represents a double-edged sword: large amounts of data mean that marketers and marketing methodologies can be better attuned to the wants and needs, and buying habits of consumers. Companies and Businesses catering to those wants and needs can then increase their efficiency and provide a better product offering. However, the obverse implication is that for anyone wanting to break through and steal the information contained within, the rewards for this piracy grow higher the more information is kept.

These figures show that there is without question a market for e-commerce. What's holding it back? Customer trust.

In order to responsibly and aggressively leverage the potential that e-commerce represents, the Information Technology industry must show that it is respecting the rights of individuals, and enacting policies, procedures and best practices that entrench those rights in the very technology used to conduct business, whether on line, in a database, or on a smart card. Industry convergence is quickly making these technologies, and many others, interoperable. If the technologies are interoperable, then the information contained within can also be shared. Without the proper safeguards such as mentioned above and discussed in this paper, what assurances do consumers or citizens have that they are not giving away their most precious possession, their identity?

## 2. Background

During the last fifty years, advances in computer technology have made possible the compilation and sharing of detailed information. The use of advanced databases and Information Technology in general has heralded a new way of looking at how information is stored, accessed, shared and retained. As these advances in computer technology continue, however, it is incumbent on the keepers of these information warehouses to protect against the misuse of the information they keep. Without trustworthy guardians, who would supply information about themselves?

Over the last twenty years, a plethora of Privacy related regulations and legislation has been passed, including the Canadian Standards Association's Model Code for the Protection of Personal Information<sup>v</sup>, the Privacy Act of 1983, and in the U.S., the Identity Theft and Assumption Deterrence Act of 1998, Children's Online Privacy Protection Act 1998, and the Graham-Leach-Bliley (GLB) Act.



***Delivering the Future . . . Prescient Solutions.***  
***[www.prescient.net](http://www.prescient.net)***



These examples of legislation are aimed at protecting the rights of the citizen, while ensuring the balance of business to carry on its ability to generate revenue and profits.

The real issues of Privacy have only become paramount in the last few years, coinciding with the rise in the use of the Internet for ubiquitous communications.

Due to the proliferation of individual's data across enterprise organizations, government, service providers and business entities, the need for solid Privacy Enhancing Technology has moved from an antithetical issue with respect to business, to one that can allow the increase and growth of business.

As online business transactions continue to grow, and more and more organizations capture and retain information in an electronic format, protecting the privacy rights of users, consumers and citizens keeps getting pushed to the forefront of the discussion. Most privacy policies are intended to be technology neutral. However, because of the ways in which some Privacy Enhancing Technologies can execute the stringent and exceptional protection of personal privacy, it is possible that technology-neutral policy could actually fall short of protecting personal information—as it is stored in electronic format.

The Encrypted Relational Database Model (**ERDM™**) as developed by Prescient International, for example, is one such case.

The **ERDM™** takes privacy to a data level by encrypting the relationships between data elements, and by making data management possible without compromising the information stored within the database.

By employing this database architecture, organizations can prove to customers and citizens (in the case of government) that they are proactive in maintaining Privacy, Security and Confidentiality. As well as being a business imperative, this is also being legislated to stronger and stronger degrees. For businesses and organizations to show that they are able to meet the growing demands placed on electronic documents-management, the use of stronger and stronger Privacy Enhancing Technology is a must.

### 3. Issues with Lack of Privacy

Key issues that arise when privacy is not maintained are Identity Theft, Fraud, violation of rights, and distrust of guardians.

Between January 2000 and December 2000, 31,103 cases of Identity Theft were reported to the Federal Trade Commissioner's office in the US<sup>vi</sup>. That number compares to 69,370 for the period from November 1999 to June 2001<sup>vii</sup>, suggesting



***Delivering the Future . . . Prescient Solutions.***  
***[www.prescient.net](http://www.prescient.net)***



that the frequency with which this type of fraud is being committed is increasing quite dramatically.

The results of Identity Theft can include temporary and sometimes-permanent financial loss from tax refunds, liens or owed monies. The damages can also extend past direct damages to indirect repercussions, including denial of credit, loans, social service benefits or other government programs and services, home services such as utilities and telecommunications or even housing in an apartment if the landlord decides to run a credit check.

Being able to track and identify where an individual is located is also an issue with enhanced technology. As devices such as cell phones, which send out a locator signal every ten minutes or so, and other wireless devices that transmit and receive information become more ubiquitous, the concerns surrounding access to personally identifiable information are heightened.

Location-based services, such as cell phone use, have the potential to pinpoint where a user is within almost any given area (where a signal is received). This could imply a distinct threat to privacy protection, in as much as an individual can be identified, and tracked, based on information that is being gathered for the delivery of a service (such as cell phone use). Emergency services, however, are in the precarious position of needing enhancements to their service delivery<sup>viii</sup> that cross over this border of service delivery and invasion of privacy.

Further, many cases exist where trusted users have betrayed their positions of trust, and have exploited the information at their disposal<sup>x</sup>. Even inadvertently, examples of database privacy breaches are becoming more commonplace. Often, it is simply due to the fact that the *de facto* standards are no longer sufficient for protecting privacy<sup>x</sup>.

## 4. What is Privacy?

Privacy is the ability for a person to control the information relating to them, including the collection, use and disclosure of that information.

Security is the protection of that information.

Confidentiality is the principle that supports the obligation of an organization to understanding the risks associated with keeping that information about others safe, and not to misuse or disclose that private information without proper consent.

Privacy protection is not simply being able to opt out of services such as points programs, but rather, it extends to the control of information held within an organization, whether that organization is a form of government, or a business.



***Delivering the Future . . . Prescient Solutions.***  
***[www.prescient.net](http://www.prescient.net)***



Central to this issue is the question of “who gets what access to what information.” This can be seen most clearly in the case of a systems’ “superuser” who has the rights to assign access privileges for the entire system. Because of the way in which most network and database management is carried out, there is a distinct threat of these internal resources having access to all information, and being able to copy, download, steal or sell any information contained within the electronic storage system.

Governments are responsible for maintaining the privacy and confidentiality of its citizen’s records. Canada’s Personal Information and Protection of Electronic Documents Act for example, binds businesses, such as banks, airlines and telecommunications companies. Similar legislation in the U.S., such as the Graham Leach Bliley Act governs the use, disclosure and retention of information for the purposes of electronic commerce. The list of legislation, regulations and amendments is long, and growing. The fact is that Privacy is not an add-on, but rather it is now being viewed more and more as a predicate to business transactions.

The notion of Privacy is based on what society determines an individual is. One individual is separated from another by the responsibilities, privileges and courses of action that they take throughout their lives. Much like in a large organization, the roles and responsibilities of one person dictate and determine how they are identified within that organization’s hierarchy. Rights of access, duties and rewards all stem from the ability of the organization to determine what that particular individual has done, and what they are responsible for.

Imagine an organization, a large corporation for example, where no workers could be identified, where one person’s duties and responsibilities could not be separated from another’s. This would lead, predictably, to anarchy—or at best, some form of communistic dogma. In a capitalistic sense, this would lead to gross inefficiencies and lack of productive work.

In an environment such as a free and democratic society, the example above presents some different complications. If no one citizen is able to prove, definitively, who they are and what they’ve done, then the entire democratic infrastructure begins to crumble; a lack of privacy in a democratic society means an erosion of self-sustaining development. A lack of identity means a lack of accountability. A lack of privacy protection leads to the same conclusion; without protection of privacy for all citizens, those who chose to subvert the law can do so with relative impunity by stealing valuable information about specific individuals—information that belongs to those individuals.

Privacy, as a moral principle of commerce and democratic social cohesion, is imperative to the sustainability of growth. As modern western societies and their



***Delivering the Future . . . Prescient Solutions.***  
***[www.prescient.net](http://www.prescient.net)***



Information Technology infrastructures become more and more intertwined, the protection of privacy is paramount to being able to continue a robust and healthy economy.

More importantly, because democracy is not a guiding principle that has been discarded in modern western societies, the rights of those citizens who do not want their information shared, distributed or used still carry more weight of those who would rather have an identity-neutral society where no one person can be distinguished from another, and where all identities are effectively interchangeable.

Privacy protection is an issue that must be treated as an *extrinsic telos*—a journey, rather than a destination.

## 5. Difference Between Security, Privacy and Confidentiality

There has been a lot of discussion within the Health industry with respect to the privacy of patient and confidentiality data. Most of the discussions end up with reference to security measures and policy for the accountability. However, there is a marked difference between Security, Privacy and Confidentiality. As clearly outlined by the Privacy commissioner of Canada, in his speech "E-Health 2001: The Future of Health Care in Canada"<sup>xi</sup>,

"I often wish the terms "security," "confidentiality", and "privacy" were not so readily bundled. The problem with always talking about them this way, as a bundle, is that they tend to get used interchangeably. People think that they are talking about privacy when what they are really talking about is security or confidentiality. That, I want to emphasize, is a mistake. They're entirely separate issues.

Privacy is our right to control information about ourselves—including the collection, use, and disclosure of that information.

Confidentiality is your obligation to protect someone else's personal information in your care, to maintain its secrecy and not misuse or wrongfully disclose it.

And security is the process of assessing and countering threats and risks to information."



***Delivering the Future . . . Prescient Solutions.***  
***www.prescient.net***



Having a clear description of Security, Privacy and Confidentiality, we should now look into Privacy Enhancing Technology.

## 6. Privacy Enhancing Technology - What is it

Privacy Enhancing Technology is an industry-specific phrase that refers to technology that assists in the protection of privacy. This could include anything from biometrics or a smart card to database models that prevent unauthorized access to information held within.

Privacy Enhancing Technology is like a lock on a policy. It cannot work unless there are a number of other protocols and support mechanisms; no Privacy Enhancing Technology can work in exclusion of its best practices, just as no key will work without a lock to secure or undo.

Furthermore, Privacy Enhancing Technology is also a tool to prevent the caretakers or administrators or custodians of the data from gaining access to information, unless explicitly authorized through policy or through delegation.

To further the cause of privacy Prescient developed Encrypted Database Relational Model (**ERDM™**), a Privacy Enhancing Technology.

## 7. Description of ERDM™



When dealing with personal and confidential information in an electronic format, there exists, by default, access rights that are granted to Systems and Database Administrators. These rights are legitimate as they are required for the purposes of operations and management of systems. For example, under Ontario's **FIPPA** (Freedom of Information and Protection of Privacy Act) and **MFIPPA** (Municipal Freedom of Information and Protection of Privacy Act) however, such Administrators should not have the right to view or access confidential personal information, which could then be used to identify an individual.

An area where privacy concerns are becoming increasingly paramount is the health industry. With the goal of providing patients better access to health care from anywhere they choose, to creating and maintaining thorough medical records, this industry is moving towards an Electronic Service Delivery Model. With this new model, sensitive patient information is exposed unless essential privacy and security issues are not addressed.

In order to ensure privacy and confidentiality of patient data, a number of issues need to be considered. Access rights and storage of confidential information are vital issues. Furthermore, mitigating the threat of unauthorized access both from within an organization and from beyond also needs to be paramount to any



*Delivering the Future . . . Prescient Solutions.*  
[www.prescient.net](http://www.prescient.net)



solution. Solutions that do not succeed in addressing these fundamental issues will ultimately fail in protection of confidential data.

Prescient International has developed a tool for Privacy Enhancement. When used in the Health Care applications, the Encrypted Relational Database Model (**ERDM™**) represents a new method of application and data design and management that ensures privacy and confidentiality of patient records, effectively de-coupling patient information from medical information. With the implementation of **ERDM™**, neither Systems nor Database Administrators will be able to compile pieces of confidential information on any patient, such as tombstone data (e.g. date of birth, etc.), which could then be used to identify an individual. This solution prevents unauthorized access and ensures that patient data is secure, while reinforcing the fundamental tenets of legislation and societal trust in a public health system.

In order for a malicious hacker to access information that can identify a person, a specific query must be run, such as an SQL (Structured Query Language) query. These queries are similar to a logical statement that has specific qualifiers affecting operators and modifiers such as "if," "what," "and," etc. The difference between traditional relational databases and Prescient's Encrypted Relational Database Model is that an administrator (like a DBA or a Systems Administrator) cannot create a qualified query, since no known direct relationship exists between the entities. Therefore, relationships between data entities are secure, even from Systems and Database Administrators.

Recent articles in the news have highlighted issues of privacy and confidentiality with stories on hackers getting access to personal files and raw patient data<sup>xii</sup>. Changes to legislation at both the federal and provincial level in Canada, as well as at the State and Federal level in the U.S. are attempting to react to these issues by ensuring that the rights of citizens are entrenched, and that the law protects the privacy and the confidentiality of personal information. Prescient has anticipated the results of such legislation by developing this relational model that prohibits the compiling of sensitive raw data elements without blocking authorized access. This means that doctors and other authorized health care providers can access confidential patient data, but that no one who is unauthorized will be able to identify or use this confidential information. Queries can still be run on the data itself, for example, numbers of patients with high blood pressure, or the number of a certain kind of prescriptions that have been filled, but the relationships to personal qualifiers and identifiers are encrypted, meaning that confidential data is secured.



***Delivering the Future . . . Prescient Solutions.***  
***[www.prescient.net](http://www.prescient.net)***



## 8. Benefits of ERDM

Since Privacy is one of the corner stones of a progressing society, the benefits are wide and varied.

Primarily, the main benefits of the **ERDM™** are the strong protection of Security, Privacy and Confidentiality within an electronic format. While treating each one of these issues as distinct, the **ERDM™** addresses the issues inherent in each distinct area.

Without question though, the biggest advance and benefit that can be derived from the **ERDM™** is that if the security of any one single part of the database is breached, the rest of the database is not at risk. As well, because Privacy is integrated into the data itself, no "back-door" exists through which administrators or unauthorized users could potentially gain access.

## 9. Prescient Background

"**Prescient**" - pres-ci-ent; English definition: intuitive, clairvoyant, psychic, foresees the future "We have the prescient ability to envision Information Technology of tomorrow, today."

"PI" - mathematical equation used in numerous angular calculations:

$$22/7 = 3.142857114285711428571$$

"Never ending, undivisible."

Since 1995, Prescient International Inc. has been on the leading edge of Business and Information Technology innovation in Ontario and around the world. Projects ranging from bold and original network design to award winning applications have brought Prescient accolades and the highest client satisfaction. Prescient has consistently led the way with ahead-of-the-curve design and implementation.

*Out-Of-The-Box Thinking, Vision, Innovation, Guaranteed On-Time Delivery and Total Client Satisfaction* are the hallmarks of Prescient's commitment to our valued clients.



***Delivering the Future . . . Prescient Solutions.***  
***www.prescient.net***



Prescient understands today's evolving, competitive environment and we design solutions to seize the opportunities created by this new environment. We take pride in continually staying on the leading edge of industry trends through regular training, memberships to various standards bodies, and constant exposure to new technologies. As a result, we apply the latest skills and methodologies to meet your needs for today and tomorrow.

## 10. Case Use - ERDM in Electronic Health records

The Encrypted Relational Database Model is being currently being implemented in an Electronic Health Management System (**EHMS™**).

The **EHMS™** is a web-based, browser independent and device-independent, comprehensive Practice and Clinical Management system, allowing physicians to access information securely from anywhere, anytime, thereby maximizing efficiencies in the delivery of optimal health care. Created in close collaboration with physicians, the result is a user-friendly interface that allows interaction with the system through any method of input; point and click, free text entry, a combination of the two, voice recordings, image drawings, and handwriting. It provides physicians with intuitive usability at varying levels of functionality, based on the physician's needs and technical comfort.

Through the **EHMS™**, physicians have a secure, effective means of data management. The application enables physicians to provide quality, longitudinal care to patients through the long-term storage of patient information. The **EHMS™** incorporates leading edge health information and guidelines released by National and International Health Agencies into discrete disease modules that can be applied to the stored patient information. Based on the patient's current state of health, past history, family history, physical measurements and medication history, the **EHMS™** provides the physician with information and decision support tools at the point of care for the optimal management of patient care.

Through the automating of administrative functions practice management tasks are handled with a few clicks. Routine processes such as scheduling are made efficient by allowing one scheduler to be utilized for any number of physicians within an office and between offices. The scheduler even checks for available appointments at referring physician offices reducing the time spent on booking appointments for patients and staff.

Billing functions are completed in a fraction of the time and automating this task greatly reduces human error. The **EHMS™** simplifies individual billing and group



***Delivering the Future . . . Prescient Solutions.***  
***[www.prescient.net](http://www.prescient.net)***



billing and checks claims for validity before they are sent for processing. The **EHMS™** is designed to interface with various electronic billing systems resulting in more efficient processing of claims.

The **EHMS™** provides this functionality at no cost to speed and performance, enabling timesavings for physicians in their day-to-day activities and therefore, enables them to spend more time with their patients in the provision of optimal care.

Although the merits of the electronic management of information are numerous, a major concern lies in the security and privacy of data. Electronic information can be intercepted and altered easier than its paper-based counterpart. It can be copied and used for purposes unknown to the person who supplies it. Keeping business and patient records secure in this new, connected environment poses a challenge. In order to protect the rights and privacy of patients' electronic information, major forces based on market demands and regulations are calling for the development of enhanced security policies and practices. As a result, ironclad security and privacy of patient medical information is now mandated by legislation.

The bond between a patient and physician is tightly bound by trust - trust that a patient's information will not be mishandled or mistreated in any way, thereby compromising their confidentiality. Organizations often take a reactive approach to system security rather than a proactive approach; implementing safeguards for information protection after security has been breached. This demands that security should be integrated from the early stages of inception through to the implementation of organizational systems. Prescient's **ERDM™** and **e<sup>2</sup>Sec™** provide organizations and individuals a total end-to-end secure environment.

**ERDM™** and **e<sup>2</sup>Sec™** surpasses technologies currently on the market by providing an end-to-end secure environment to ensure complete patient and physician security, privacy, and confidentiality from within and beyond the organizations involved. A patient who consents their physician to collect and maintain their data, through the application, can be assured of complete security, privacy and confidentiality using the **e<sup>2</sup>Sec™** and **ERDM™**.

## 11. Conclusion

Privacy is not a privilege it is a right. In order for companies to do business in the global environment that is electronic services, adherence to Privacy principles is mandatory. Even if an organization, such as a Small to Medium Enterprise, is keeping its employee records on a server, there are inherent issues to the collection, use, disclosure and retention of those documents.



***Delivering the Future . . . Prescient Solutions.***  
***[www.prescient.net](http://www.prescient.net)***



As businesses, organizations and governments move forward into the 21<sup>st</sup> century and the use of Information Technology becomes more and more ubiquitous, the need for stringent Privacy Enhancing Technology will continue to surface. Without proper safeguards in place, not only is the information being held by an organization at risk, but so is the ability of that organization to carry on its operations.

For more information on Privacy:

Privacy Commissioner Of Canada's website:

<http://www.privcom.gc.ca>

Information Privacy Commissioner of Ontario's website:

<http://www.ipc.on.ca/>

Other Canadian Privacy Oversight bodies:

[http://www.privcom.gc.ca/information/comms\\_e.asp](http://www.privcom.gc.ca/information/comms_e.asp)

Federal Trade Commission website:

<http://www.consumer.gov/idtheft/>

Federal Trade Commission Hotline:

1-877-ID-THEFT (438-4338)

Center for Democracy and Technology

<http://www.cdt.org/>

EPIC Electronic Privacy Information Center

<http://www.epic.org/>

---

i "Meeting New Standards for Managing Privacy of Health Information Canadian Institute", speech by George Radwanski, Privacy Commissioner of Canada June 18, 2001 Toronto, Ontario to: Condition Critical: Health Privacy in Canada Today

ii April 23, 2002 Ottawa, Ontario Information, Privacy, and Security, George Radwanski, Privacy Commissioner of Canada

iii The Daily, Statistics Canada, April 3, 2001

iv ibid

v the CSA Model Code's Ten Privacy Principles are: Accountability; Identifying Purposes; Consent; Limiting Collection; Limiting Collection, Use, Disclosure, and Retention; Accuracy; Safeguards; Openness; Individual Access; Challenging Compliance

vi "Identity Theft Victim Complaint Data" presentation, Federal Trade Commission's Identity Theft Data Clearinghouse January 2000 to December 2000, <http://www.consumer.gov/idtheft/reports.htm>



***Delivering the Future . . . Prescient Solutions.***  
***[www.prescient.net](http://www.prescient.net)***

---

vii *ibid*; November 1999 to June 2001

viii The FCC's wireless 911 rules seek to improve the reliability of wireless 911 services and to provide emergency services personnel with location information that will enable them to locate and provide assistance to wireless 911 callers much more quickly. To further these goals, the agency has required wireless carriers to implement E911 service, subject to certain conditions and schedules. The wireless 911 rules apply to all cellular licensees, broadband Personal Communications Service (PCS) licensees, and certain Specialized Mobile Radio (SMR) licensees. Wireless carriers are required to provide Automatic Location Identification (ALI) as part of Phase II E911 implementation beginning October 1, 2001. Enhanced 911 (E911) is a service that automatically locates the caller for dispatch. The FCC's new rules require wireless carriers to log and track where customers are, to enhance the speedy delivery of emergency services. For additional details about the FCC's Enhanced 911 rules, see <http://www.fcc.gov/911/enhanced/>.

ix In March of 2002, the New York Electronic Crimes Task Force issued a Press Release about a recent sting operation that they had carried out. An employee of the Prudential Insurance Company, Donald Matthew McNeese, who was a database administrator, was arrested and charged for identity theft, credit card fraud and money laundering charges. As the administrator, McNeese, it is alleged, downloaded personnel records for as many as 60,000 Prudential employees throughout the United States. He was apprehended during a sting operation that caught him, among other things, trying to sell Prudential employees' identities over the internet. See: <http://www.usdoj.gov/usao/nye/pr/2002mar01.htm> for full press release. The successful apprehension of the accused stands as an excellent example of successful cooperation between law enforcement and private industry; the United States' Attorney thanked Prudential Insurance Company for their assistance and full cooperation in the investigation.

x "Choicepoint, a database firm that sells information about individuals and companies to clients, including the FBI and insurance firms, left an internal corporate database viewable to anyone with a Web browser, the company confirmed," article on [www.wired.com](http://www.wired.com), 1:40 p.m. Jan. 22, 2002 PST.

"The private medical files of thousands of Ontario patients have been stored on-line where they're vulnerable to hackers and the prying eyes of government-hired technicians, according to documents obtained by The Globe and Mail. Less than a month after the Health Ministry set up a much-vaunted patient-information database for doctors, Ontario's privacy commissioner is investigating the system for breaching one of the most sacred tenants of medicine: doctor-patient confidentiality. The commissioner is looking into a wide range of allegations, from whether private companies have been given access to patient information to whether some of the information has already been lost." Graeme Smith, *Globe and Mail*, Monday, December 10, page A1

xi May 29, 2001 Toronto, Ontario: Patient Privacy in the Information Age by George Radwanski, Privacy Commissioner of Canada

xii see endnote ix and x

