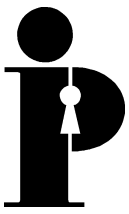
Information
and Privacy
Commissioner/
Ontario

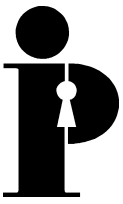
# Submission to Industry Canada's Electronic Commerce Task Force

## A Cryptography Policy Framework for Electronic Commerce

## Building Canada's Information Economy and Society



Ann Cavoukian, Ph.D.
Commissioner
April 21, 1998



**Information and Privacy Commissioner/Ontario**

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

This publication is also available on the IPC website.

# Table of Contents

# 1. General Considerations

Privacy, confidentiality and security have become pivotal issues in the attempt to provide the legal, policy and technical framework for the wide diffusion of electronic commerce, and more generally for the wider acceptance of the Internet, in Canada and internationally. A broad consensus has emerged that recognizes that there must be public trust and confidence in open networks before a majority of the public and businesses will be prepared to engage in electronic transactions.

The public rightly perceives that open communication networks such as the Internet are subject to vulnerabilities that increase the threat of personal data being accessed without consent, misappropriated, altered, or destroyed.

Cryptography is seen as a technology that has the necessary features to ensure the confidentiality and privacy of personal data communicated or stored. The ability of encryption to prevent unauthorized access to plaintext is this technology's strongest feature, providing users with the assurance that their communications cannot be intercepted by third parties. The incentive to use encryption for communications over open networks is predicated on the unassailable integrity of the encryption process. Public confidence in encryption will rest on its ability to deliver strict confidentiality.

Proposals to allow for lawful access to encrypted data would create a fundamental derogation from the very purpose for which this technology is employed. Incentives to use the technology may well diminish if it came to be generally understood that encrypted data could be subject to lawful third-party access.

# 2. Scope of Comments

Electronic commerce encompasses a variety of transactions between different parties, including business to business, business to government and business to consumer transactions. From a privacy or data protection perspective, the latter type of transaction is the one where the issues of security, confidentiality and privacy are most focused.

While business to business and business to government transactions also require security and confidentiality, only business to consumer transactions must deal with the additional issue of privacy.

# 3. Data Protection Principles

Canada is a signatory to the OECD Guidelines on the Protection of Privacy and Transborder Dataflows and other international covenants that protect privacy, and has adopted both federal and provincial privacy or data protection legislation. Moreover, a model privacy code has been developed for the private sector by the Canadian Standards Association based on the data protection principles found in the OECD guidelines and in the privacy laws across Canada.

These statutory and voluntary rules create the conditions for the diffusion of cryptography, particularly strong encryption, as part of the Canadian privacy infrastructure. This infrastructure will be further augmented when the federal government adopts data protection legislation for the federally regulated private sector.

Encryption can be viewed as an essential technical mechanism that complements the existing, and future, legal and policy framework.

# 4. Lawful Access

Given that strong encryption can play a significant role in ensuring confidentiality and privacy in open networks, and that for electronic commerce to thrive, an environment of trust needs to be created in electronic transactions (which can only be fostered in the presence of confidentiality and privacy), can an argument be made for lawful access to decrypted text?

As stated in the consultation paper:

> Today, strong encryption is increasingly being used by businesses and individuals, and strong cryptography is increasingly available in shrink-wrapped mass market software or public domain "free-ware" on the Internet. There is a growing global demand for cryptography products, and design and manufacturing capabilities are emerging in many nations. At the same time, law enforcement agencies and national security agencies are concerned that the widespread use of strong encryption without some capability for lawful access will significantly impact upon their investigative capabilities.

Public opinion polls over the last several years show that the vast majority of North Americans have serious concerns about their privacy, and are very cautious about entering into financial transactions over the Internet, particularly when they are asked to provide personal data and other information such as credit card numbers.

The basis of their concern is not just the recognized security vulnerabilities associated with open networks, but also the intrusiveness of the technology in being able to collect personal information surreptitiously. The economics of personal information are now such that personal significant commercial value. 'Capturing' personal information has become an industry worth billions of dollars, creating the economic incentive for the collection, use and disclosure of personal data.

Apprehension about the collection, use and disclosure of personal information via the Internet can only be diminished by deliberate policies, regulations and privacy enhancing technologies that have as their objective, the protection of personal information. Encryption is such a privacy enhancing technology.

The predicament faced by government wishing to introduce lawful access to decrypted information is that such an approach could potentially undermine the cryptographic technology itself and therefore, its privacy and confidentiality benefits, which would in turn undermine public confidence in the use of the technology. In addition, the perception that lawful access would become embedded in the technology may convince users that they have no wish to use a technology that could subject them to constant monitoring and surveillance. If this is a possible outcome of lawful access, then government policies to encourage the use of cryptography would be in fundamental conflict with government support for lawful access.

# 5. Key Recovery

Lawful access by law enforcement and security agencies is predicated on the ability of these agencies to recover the 'secret key,' in either a symmetric or asymmetric key infrastructure, allowing them to read the decrypted text. For government, the issue is whether it will seek to legally mandate that all encryption technologies include key recovery mechanisms before such products are sold to the public.

# 6. Options

The consultation paper raises a number of options on how the government could proceed on the issue of key recovery.

## 6.1. Real-Time Communications

Encryption of real-time communications would entail the encryption of the message 'in-transit' through the Internet or other open communications systems. Once read, the message would then be either destroyed or archived. If lawful access was required for the archived message, it could be retrieved some time after the message was received and when the private key was obtained under a court order, assuming that the message was archived encrypted. This procedure would operate as it is done presently with any lawful access to records.

If, however, lawful access was required for the actual 'in-transit' communication, then the procedures to implement such an interception could become problematic. Ordinarily, there is little need from a business point of view to require key recovery for real time communications, since the message is decrypted at both ends. If, nevertheless, lawful access is mandated, a number of problems would arise that would greatly complicate the ability of law enforcement agencies to gain lawful access. To be effective, access would have to be timely, a few hours after the transmission at the latest, and to achieve this quick turnaround time, the interception of the 'in-transit' encrypted message would have to be made before the content of the message was decrypted. A third party would have to hold the user's secret key since access through the user would alert the user. Then there is the issue of evidence. Until decrypted, the 'in-transit' message would have no evidentiary character, but the process of decryption would require court authorization.

The consultation paper recognizes the difficulty posed by these conditions when it states that, "it would be difficult to determine whether the information being intercepted fell within the scope of the legal authorization to intercept it." Access to the decrypted information would be first required before such an assessment could be made. Under these conditions, the law enforcement or security agency would require permanent access to the 'in-transit' communication, but could not decrypt it without a court authorization.

However, any attempt at creating a seamless and on-going ability to engage in lawful access to the 'in-transit' communication would likely be subject to scrutiny under the Charter of Rights and Freedoms. From a privacy perspective, such a procedure would violate most of the existing data protection principles. Indeed, the potential exists for lawful access to turn into massive 'fishing expeditions.' In this scenario, the balance between the interests of law enforcement, civil liberties and privacy would be struck largely in favour of law enforcement.

On the basis of these considerations, mandatory controls imposed by government could create a 'chilling effect' on the use of encryption for real-time communications, since it could be perceived that the balance between law enforcement and confidentiality/privacy had been struck too greatly in favour of law enforcement. Secret monitoring and surreptitious access to private keys would create the conditions for a 'surveillance society.'

**Recommendation 1:**

**That the government adopt a cryptography policy that does not mandate that lawful access mechanisms be embedded in hardware or software, and that does not prevent users from employing products that do not possess key recovery features.**

## 6.2 Stored Data

It has been generally recognized that key recovery in the context of stored data can be justified from a business point of view. A company or individual would want to be in a position to recover valuable business data, if that data was encrypted by an employee who, for whatever reasons, was not available to provide the secret key. However, such a key recovery problem could be dealt with internally, through an internal key management system, with little or no need to involve an outside third party.

A government requirement that companies or individuals deposit their secret keys with a central body — a trusted third party, through which there would be lawful access on a continuing basis would create numerous problems.

1. There is a risk to the user that a complicated key recovery mechanism could create various vulnerabilities to the encryption system itself, thereby undermining confidentiality and the security of the encryption system.

2. The proposed key recovery system is more complex than the encryption system itself and would be less transparent to users, who may then not wish to use the system.

3. If key recovery is lodged with a central third party over which users of encryption have no control, confidence in the system could be undermined.

If lawful access is required, it would be less costly and less complicated to rely on the key recovery mechanisms that businesses would adopt for their own purposes. This approach would also be consistent with civil liberties and privacy principles, since it would not create a permanent mechanism for surveillance.

**Recommendation 2:**

**That the government adopt a cryptography policy that is market driven, with the government encouraging back-up encryption keys and setting minimum standards for the use of data or key recovery.**

## 6.3 Digital signatures

Since digital signatures are used for purposes of identity authentication, data integrity and non-repudiation, and not for confidentiality of data, there would be no need for a key recovery mechanism for digital signatures.

**Recommendation 3:**

**That the government adopt a cryptography policy that does not include digital signatures in a mandated key recovery system.**

## 6.4 Trusted Third parties

If trusted third parties are created, they will need to be regulated to ensure that they adhere strictly to accepted privacy principles and practices. Failure to regulate trusted third parties could lead to a failure of the key recovery system to guarantee security, confidentiality and privacy.

**Recommendation 4:**

**That the government adopt a cryptography policy that binds trusted third parties to strict privacy principles and practices.**

# 7. Conclusion

It is our view that the proper balance between lawful access, privacy and confidentiality is one that does not include mandatory controls that permit law enforcement and security agencies to gain embedded technological access to decrypted information or data.

# 8. Summary of Recommendations

## Recommendation 1

That the government adopt a cryptography policy that does not mandate that lawful access mechanisms be embedded in hardware or software, and that does not prevent users from employing products that do not possess key recovery features.

## Recommendation 2

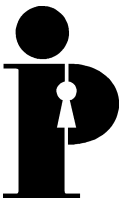
That the government adopt a cryptography policy that is market driven, with the government encouraging back-up encryption keys and setting minimum standards for the use of data or key recovery.

## Recommendation 3

That the government adopt a cryptography policy that does not include digital signatures in a mandated key recovery system.

## Recommendation 4

That the government adopt a cryptography policy that binds trusted third parties to strict privacy principles and practices.



**Information and Privacy Commissioner/Ontario**

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca