
Cryptography Policy Discussion Paper: Analysis of submissions

Prepared by



AEPOS Technologies Corporation

PREPARED FOR : Industry Canada

ORIGINATOR : AEPOS Technologies Corporation
116 Albert St. Suite 601
Ottawa, Ontario
K1P 5G3

DATE: 11th June, 1998

This publication is also available electronically on the World Wide Web at the following address:

<http://strategis.ic.gc.ca/crypto>

This publication is also available in alternative formats on request.

See distribution contact numbers listed below.

For additional copies of this publication, please contact:

Donna Emmett
Task Force on Electronic Commerce
Industry Canada
300 Slater Street, Room 2022A
Ottawa, Ontario
K1A 0C8

Tel.: (613) 990-9233
Fax: (613) 941-0178
Email: emmett.donna@ic.gc.ca

Michael Harrop may be contacted at:

AEPOS Technologies Corporation
116 Albert St., Suite 601
Ottawa, Ontario
K1P 5G3

Tel.: (613) 599-5905
Fax: (613) 599-4681
Email: mharrop@bigfoot.com

©Her Majesty the Queen in Right of Canada (Industry Canada) 1998
Cat. No. C2-336/2-1998
ISBN 0-662-63949-9

Table of Contents

Introduction	1
General observations on the comments received and the process of analysis	3
Analysis of responses	5
Part 1: Summary of quantitative results	5
Overall position towards controls on cryptography	5
Encryption of stored data	6
Encryption of real-time communication data	7
Export controls	9
Part 2: Review of narrative responses	10
General observations	10
Mandatory key recovery/key escrow issues	10
Access to stored data	12
Real-time communications data recovery	12
Cost issues	13
Privacy issues	13
Law enforcement issues	14
Export Controls	16
The need for suppliers and carriers to be treated equally	17
Legislation, regulation and Charter issues	17
Other issues	18
Conclusions and possible follow-on actions	19
Part 3: Suggestions for expediting the rollout of secure electronic commerce ...	20
Legal issues	20
Trusted Third Parties	21
Lead by example	21
Security for electronic commerce	21
Role of government in promoting the electronic services	22
International issues	23
Closing remarks	24
Annex A: Resolution of the Association of Canadian Chiefs of Police, August 1997 .	25
Annex B: Index of Submissions to the Discussion Paper	26

Introduction

This report contains an analysis of the responses to the Industry Canada discussion paper *A Cryptography Policy Framework for Electronic Commerce* (February 1998). The paper was released for public comment on 21 February, 1998 with a comment closing date of 21st April, 1998. A total of 189 responses were received by the closing date. A further 15 responses were received between the closing date and 22nd May.

In addition to comments in response to the discussion paper, responses included requests for more information, e-mails and letters acknowledging receipt of the discussion paper, e-mail advertising (spam), messages that appeared not to have any relevance to the topic (such as a request for help with a consumer problem), duplicate copies of submissions submitted by different delivery mechanisms and at different times, and faxed cartoons. These responses were not included in quantitative assessment or the analysis.

Late contributions are not included in the statistical analysis but the comments have been considered and taken into account in the evaluation process.

The overall count of submissions was as follows:

Total on-time responses:	189
Responses not analysed (see above):	53
On-time submissions analysed:	136
Late submissions:	15
Total responses (as of 22 nd May, 1998):	204

The submissions received represent a broad cross section of interest. In addition to 77 responses from private individuals and academics, submissions were received from 13 supplier/manufacturer companies, 18 law enforcement agencies from all parts of the country, four public sector agencies (including the offices of three Information and Privacy Commissioners), five industry associations, five privacy/human rights organizations, five carriers or carrier associations, five consultants and four other organizations. The carrier associations represented all provincial telephone companies plus some of the wireless companies. The industry associations included representation for Canadian financial institutions across the country, 110 Internet service providers, over 3500 manufacturing and exporting companies, the telecommunications user interests of over 400 businesses, governments and healthcare providers with an aggregate total of over 2 million employees, and over 1300 computer hardware, software and service companies with revenues in excess of \$45 billion and over 290,000 employees.

A number of submissions arrived indirectly. These included 14 individual letters that were addressed to Industry Canada as responses but which accompanied the Electronic Frontier Canada submission and some submissions from law enforcement agencies which were addressed to the RCMP, the Ottawa Carleton Police Force and the Ontario Solicitor General, rather than Industry Canada. Each of these contributions has been included as a distinct submission. In addition, a single letter signed by 20 international organizations concerned with defending civil liberties and human rights on the Internet, was included with the Electronic Frontier Canada submission. For analysis purposes, this letter was considered as part of the Electronic Frontier Canada submission, rather than being identified as a separate contribution.

Submissions varied in length and detail from very short individual e-mails that protested about any kind of government control to very substantial formal submissions developed by committee. All responses judged to have any relevance to the discussion have been included in the analysis regardless of origin, tenor or level of detail.

Eight of the contributions, including that of one carrier association, expressed concern and disappointment that the discussion paper seemed slanted towards meeting law enforcement needs to access electronic information. It was suggested that there should be more emphasis on the positive aspects of cryptography and on protecting individual rights than on placing restrictions on individuals and businesses. Several comments were also made on the use of the term *lawful access* in the policy paper, observing that this is a euphemism for law enforcement access, since all crypto systems allow lawful access to their legitimate users.

A number of respondents thanked Industry Canada for presenting the issues in a public discussion paper and for giving them the opportunity to participate in the discussions. The thoroughness of the coverage of the discussion paper was frequently praised. Some respondents offered clarifications, elaborations and corrections and a number of respondents protested that the review period had been insufficiently long. Overall, the comments on the discussion paper and the process were quite favourable with most respondents appreciating the opportunity to participate in this policy development process.

General observations on the comments received and the process of analysis

Before moving on to analysis of the responses on the individual questions, a few words on the general approach and process used to evaluate the comments are in order.

As noted above, the responses varied considerably in detail and coverage. Some responses were from individuals, some from companies, some from public sector agencies, some from interest groups and associations and some from industry associations. Some responses directly addressed the issues of the discussion paper and offered answers to the questions raised while others were more of the nature of issues papers. Some responses were broad-ranging while others addressed only a single issue or a subset of the issues raised in the discussion paper. Some of the submissions provided very direct and to-the-point responses while others provided responses that were sometimes heavily masked by accompanying commentary. However, overall the responses represent a substantial amount of collective thought and effort and provide significant insight into the issues under discussion together with the considered opinions of a broad constituency. Although the analysis provided here can offer an overview into the collective thinking and opinions, the individual submissions themselves must stand as the primary response to the discussion paper.

The analysis provided in this report is partly quantitative, partly qualitative. For the most part, the submissions received comprised narrative responses to relatively open questions. Unfortunately there is no reliable or accepted way to quantitatively evaluate responses to open questions. Even the responses to the relatively closed questions (as represented by the policy options suggested under the issues of how to address encryption of stored data, realtime data and export controls), often tended to be open responses, rather than simple selection of one of the options. Thus even with the closed questions it was often necessary to interpret a narrative response as indicating one (or perhaps none) of the indicated options. Responses that said "not option 2 or 3", rather than simply indicating a preference for option 1 presented yet another challenge. Overall, the approach taken to evaluate the responses to the closed questions was to tally the responses by contributing group under each of the question headings. Where no preferred option was indicated, or where the respondent failed to comment on the issue, the contribution was excluded from the tally on that particular question. (Not all submissions responded on all the issues). The resulting assessment of the responses to the closed questions is believed to provide a reasonably accurate quantitative assessment.

Presentation of the qualitative information is much more difficult as it inevitably involves a degree of subjectivity. The approach selected was to search for those points most frequently raised and to provide a summary of the issues identified. In addition, and most subjective of all, points which, although perhaps not frequently mentioned, but which appear

to have particular relevance to the debate, or perhaps offer some new insight, have been included where appropriate.

Both quantitative and qualitative results are of value but each provides a different insight into the results. The quantitative results can provide an overall picture of stated preferences but the qualitative results, represented by the narrative responses, provide the rationale behind the stated preferences and also set out the likely implications of taking a particular direction.

Lastly, for purposes of analysis, the responses were divided into the following categories:

- Individual;
- Industry Associations;
- Law enforcement and national security;
- Privacy and human rights groups (excluding public sector);
- Suppliers/manufacturers (hardware and software);
- Carriers and carrier associations;
- Academia;
- Consultants;
- Public sector; and
- Others.

Submissions not obviously from a representative of an identifiable group, were entered as individual submissions.

Analysis of responses

Part 1: Summary of quantitative results

Overall position towards controls on cryptography

From the responses to the three specific policy options presented, it was possible to get an overall indication of how cryptography controls as a whole are viewed by the respondents from the standpoint of whether existing controls should be strengthened or lessened, or whether the status quo is preferred. The results, summarized in Table 1, indicate that 78% of respondents believe that at least some lessening of controls is justified. The 14% of respondents who believe stronger measures are justified all represent the Law Enforcement/National Security grouping. 8% of respondents indicate that, overall, the status quo is appropriate.

Respondent Group	Total Responses	More Controls	Fewer Controls	Status quo
Individual	45	0	43	2
Industry Assoc.	5	0	4	1
Law Enforcement	15	15	0	0
Privacy/Human Rights Advocates	5	0	5	0
HW/SW suppliers	12	0	11	1
Carriers & Associations	4	0	4	0
Academia	14	0	12	2
Consultants	5	0	4	1
Public Sector	0	0	0	2
Others	2	0	0	0
Total	107	15	83	9
Percentages		14%	78%	8%

Table 1: Overall position on cryptography controls

Encryption of stored data

Table 2 indicates the results of the responses to the policy options suggested for encryption of stored data.

The suggested options were: market-driven; minimum standards; and mandatory access.

Here, 52% believe that the market-driven approach is best, 29% (57% of individuals) would prefer to see no controls at all, 12% (all belonging to the Law Enforcement/National Security grouping) want mandatory access and only 6% opted for the minimum standards option. In addition, three respondents indicated that they were opposed to option three (mandatory access) but did not indicate any other preference.

Respondent Group	Total	Market	Minimum Standards	Mandatory Access	No Controls	Other Preference
Individual	51	19	2	0	29	0
Industry Assoc.	4	3	1	0	0	0
Law Enforcement	16	0	1	14	0	1*
Privacy/Human Rights Advocates	5	3	0	0	2	0
HW/SW suppliers	12	10	1	0	1	0
Carriers & Associations	5	5	0	0	0	0
Academia	14	13	1	0	0	0
Consultants	5	3	0	0	1	0
Public Sector	2	2	0	0	0	0
Others	4	3	0	0	1	0
Total	118	61	7	14	34	1
Percentages		52%	6%	12%	29%	1%

Exceptions: 3 responses indicated "not option 3"

Table 2: Encryption of Stored Data

* It was suggested that a standard form of encryption be used such that the decryption key could be made available to the authorities with judicial authorization.

Encryption of real-time communication data

Table 3 indicates the results of the responses to the policy options suggested for encryption of real-time communications data.

The suggested options were: assistance orders and selective conditions of licence (status quo); obligations on all carriers; and mandatory controls.

43% of respondents indicated that no change to current procedures (ie assistance orders and selective conditions of licence) was necessary, 25% (49% from the Individual grouping) indicated that there should be no controls whatever, 11% (all from the Law Enforcement/National Security grouping) wanted mandatory controls, 6% wanted obligations on the carriers and 5% suggested other options. Significant in the responses to this question were the 12% of respondents who explicitly objected to either mandatory controls or carrier obligations (ie respondents who declined to select one of the specified options but who indicated that options 2 and 3 were unacceptable).

Respondent Group	Total	Status Quo	Carrier Obligations	Mandatory Access	No Controls	Other Preference*
Individual	47	19.5	3.5	0	23	1
Industry Assoc.	5	4	0	0	0	0
Law Enforcement ¹	16	0	2.5	12.5	0	1
Privacy/Human Rights Advocates	5	2.5	0	0	2.5	0
HW/SW suppliers	10	7	0	0	1	1
Carriers & Associations	5	5	0	0	0	0
Academia	14	4	1	0	0	0
Consultants	4	1	0	0	1	2
Public Sector	2	2	0	0	0	0
Others	2	2	0	0	0	0
Total	110	47	7	12.5	27.5	5
Percentages		43%	6%	11%	25%	5%

Exceptions: 13 responses said "not option 3" or "not option 2 or 3"

Table 3: Real-time Communications

* Other Preference suggestions included incorporation of lawful access provisions in all public key and session key transactional applications plus support for CALEA-type legislation in Canada; non-mandatory access with three types of service - local encryption, carrier encryption, or no encryption; using a subpoena to obtain information; and rejecting the options listed without offering alternatives but without actually opposing the idea of law enforcement access.

1. Where a law enforcement response simply endorsed the resolution of the Canadian Association of Chiefs of Police (Annex A), this has been interpreted as favouring mandatory controls on the basis that the resolution calls for a mandatory key recovery regime for law enforcement access plus legislation requiring contemporaneous decryption for law enforcement access to be designed into encryption services and legislation requiring communications service manufacturers, service providers and network operators to provide law enforcement access to communications.

Note: where a response indicates that either of two options is acceptable, eg carrier obligations or mandatory access, a count of .5 has been added to each option.

Export controls

Table 4 indicates the results of the responses to the policy options suggested for export controls.

The suggested options were: relax controls; maintain existing policy; and extend controls.

Of those who responded to the question on export controls, 88% indicated they wanted to see a relaxation of the current controls (71%) or no controls at all (17%), 6% favoured the status quo and 1% (representing a single law enforcement response) specifically wanted to extend controls.

Respondent Group	Total	Relax	Status Quo	Extend	No Controls	Other Preference*
Individual	26	16	0	0	10	0
Industry Assoc.	5	4	0	0	0	1
Law Enforcement	4	0	1	1	0	2
Privacy/Human Rights Advocates	4	3	0	0	1	0
HW/SW suppliers	11	10	1	0	0	0
Carriers & Associations	4	4	0	0	0	0
Academia	12	10	1	0	0	1
Consultants	5	3	1	0	1	0
Public Sector	0	0	0	0	0	0
Others	1	1	0	0	0	0
Total	72	51	4	1	12	4
Percentage		71%	6%	1%	17%	6%

Table 4: Export Controls

* One response offered no opinion but indicated they would support a federal government decision on export controls; one said that, for their purposes, the free flow of products between Canada and the US was essential; one said we should not make changes that would put Canada out of step with the US; and one opposed any further limitations on exports and rejected the suggestion that limits might be placed on the export of products lacking key recovery.

Part 2: Review of narrative responses

General observations

The comments reflect a wide recognition of the need for strong cryptography both for business and for private use. It was noted that, in addition to electronic commerce, electronic service delivery and privacy uses, businesses need to protect themselves against industrial espionage. A number of submissions from across the spectrum expressed concern over the potential effect of policy proposals on electronic commerce and service delivery. One supplier emphasized that crypto policy must support electronic service delivery objectives, not impede them. A number of the law enforcement submissions recognized the importance of cryptography to electronic commerce but cautioned that encryption must not be allowed to shield criminal activities. The need to avoid developing a policy that was unenforceable, or that regulated only the law abiding citizen, featured in a number of responses.

Twelve of the submissions pointed out the futility of trying to impose importation or usage controls on strong cryptography which is already widely and freely available. It was broadly indicated that strong crypto will always be available to criminals, whether or not restrictions are placed on its use. The availability of non-cryptographic confidentiality techniques was another frequently-mentioned issue.

One privacy association paper listed what it considered to be a number of errors and omissions in the discussion paper. These included the risk of relying on weak encryption or systems where keys must be made available to a third party; liability issues; the infeasibility of detecting the method of encryption or even whether encryption is being used at all; the omission of any concrete evidence that the use of encryption has ever been a genuine impediment to law enforcement in any specific cases; and the omission of well known examples of improper surveillance and abuse of personal privacy.

A number of submissions remarked on the US promotion of its cryptography policy interests. Ten submissions expressed concern that Canada would simply follow the US policy directions on cryptography and indicated that this was unacceptable.

Mandatory key recovery/key escrow issues

A large number of responses spoke of the impracticality of any kind of mandatory key recovery or key escrow. Specific comments emphasizing opposition to mandatory key recovery/key escrow were included in 54 of the submissions. Of these, 26 were from individuals, five from industry associations, four from suppliers, one from a carrier/association, 14 from academia and four from other groups. Only in the law enforcement submissions was there support for additional controls to provide mandatory

access to encrypted stored data. One of the law enforcement submissions, while supporting the resolution of the Canadian Chiefs of Police, noted that mandatory access is a restrictive policy and will not work. Such controls were rejected by a large majority of respondents. Reasons advanced include the following:

- any kind of key recovery for law enforcement would create points of vulnerability and weaken the value of the encryption;
- key recovery systems are less secure, cost more and are more difficult to use;
- key recovery requirements can be evaded;
- double encryption can be used to circumvent key escrow objectives;
- non-standard algorithms can be used;
- any mandatory key recovery infrastructure will be limited in its application;
- the cost of establishing and operating a key recovery infrastructure would be high and negatively affect industry's competitiveness
- key recovery is not possible for the type of strong encryption used with smart cards.

One industry association submission noted that there was no current law to prescribe how physical data should be stored and that electronic data should not be treated differently.

Five of the submissions noted that any attempt to mandate "back door" decryption in Canadian crypto products would deter overseas buyers and disadvantage Canadian exporters.

Thirteen submissions commented on the additional points of vulnerability that would be introduced with a key escrow system and on the danger of escrowed keys being misused.

One of the carriers urged that Canada adopt a market-driven approach to strong encryption, as mandatory key recovery would put us out of step with many of our international partners.

Another point frequently made with respect to controls in Canada was that those willing to break the law would not be deterred by a legislative requirement to use cryptography with mandatory access provisions. International terrorists and criminals have access to encryption technology in the global market place. Canadians should not be prevented from protecting themselves. Controls on domestic use are widely viewed as discriminating against the honest citizen.

Several contributions highlighted the opportunities to conceal information using non-cryptographic techniques such as steganography, communicating in obscure languages and chaffing/winnowing.

Access to stored data

It was generally acknowledged that some businesses need to provide key recovery and data back-up for their own needs but it was quite strongly indicated that this should be regarded as an internal matter for business, not something to be imposed by government. It was also repeatedly indicated that any business needs in this area should not be used as a pretext to impose access requirements for law enforcement purposes. Business responses made it clear that they currently cooperate with legally authorized access requests and will continue to do so but they don't want the government telling them how to go about their business.

A number of responses suggested relying on the fact that businesses are already required to maintain certain types of record for auditing purposes and that this should suffice.

Real-time communications data recovery

Ten of the submissions (including those of three carrier/carrier associations, three industry associations, and one law enforcement agency) referred specifically to the infeasibility of having carriers or Internet Service Providers decrypt messages that have been encrypted outside of the carrier network. All the carriers/associations and two of the industry associations indicated existing methods available to law enforcement agencies are sufficient and that no additional measures are justified.

Three carrier associations and one supplier protested that the development of an infrastructure to support rapid decryption of real-time communications data would be enormously expensive, possibly in the hundreds of millions of dollars. Two of the respondents (one carrier and one association) claimed that the capability for rapid, universal decryption would have a chilling effect on the development of electronic commerce and one of the carriers noted that this would extend to the development of new encryption technologies. The term *chilling effect* was also used by one of the Privacy Commissioners in referring to mandatory controls on the use of encryption for real time communications since "secret monitoring and surreptitious access to private keys would create the conditions for a surveillance society".

Several responses noted that carriers do not retain copies of any information that passes through the network. A requirement to retain session keys would be a tremendous burden and would likely violate the *Telecommunications Act* which requires carriers to carry their customers' traffic without interference as to form or content.

One of the carrier responses noted that criminal law has never allowed officials to monitor *all* criminal communications or to seize *all* relevant criminal information.

It was also noted that, while businesses may have their own requirements for key recovery in the case of stored data, they seldom if ever have such a requirement in the case of real-time communications.

Cost issues

It is generally recognized in the submissions that any form of mandatory access provision, key recovery infrastructure or enhanced law enforcement access provisions will be very expensive. In all, 21 responses, including some from law enforcement agencies, observed on the high cost and several, including two carriers/associations, noted that the cost to business of regulated key recovery will make Canada uncompetitive internationally.

Opinions are offered by all groups on the issue of who should pay these costs. These positions can be collectively summarized in the two words "not us". Some of the law enforcement responses suggested that the carriers, suppliers or subscribers should bear the costs while some of the individual, corporate and carrier/association responses suggested that those who require the service (ie the government/law enforcement agencies) should pay.

Other cost issues were raised in the context of whether the government had done its homework in evaluating the costs, benefits and other implications of the crypto policy proposals. For instance it was noted that the differences between commercial and military/security uses of encryption have not been sufficiently defined and that cost and ease of use are not primary considerations in military/security environments as they are in commercial environments. One industry association submission urged the government not to proceed with cryptography policies or laws until an independent review has been completed to determine the cost, benefit, and risks of proposed options.

One industry association raised the issue of the costs involved in interfacing the private sector and institutional Public Key Infrastructures (PKI) to the Government of Canada PKI and recommended the costs be "reasonable, transparent and applied in a uniform manner to all PKIs, both private and governmental".

Privacy issues

Seventy-two submissions (39 from individuals, 16 from academia, 5 from privacy and human rights interests, 4 from suppliers, 3 from carriers/associations, 3 from the public sector and 2 from others) contained comments on the likely adverse impact of the policy proposals on the individual. This single issue drew more specific comments than any other. The issue of greatest concern was that law-abiding citizens would be disadvantaged by proposals to support law enforcement needs. One carrier association noted "legitimate law enforcement concerns should not be dealt with in a manner which effectively limits private citizens' legitimate use of encryption or reduces the benefits that will accrue to the private sector by

the use of strong encryption." A carrier observed that "any limits on crypto must be demonstrably justifiable in a free and democratic society" and that "measures to prohibit the use of non-accessible encryption products infringe on Canadians' right to choose and use measures they consider appropriate to safeguard their own security." Another carrier association stated that "the concerns of law enforcement agencies should not be accommodated in a manner that effectively limits legitimate private use of encryption".

A letter signed by 20 international human rights groups itemized the reasons for opposition to the policy proposals, claiming that, in their collective opinion, such policy or legislation would be "contrary to international human rights treaties, harmful to Canadian society, detrimental to the Canadian economy and in the end, simply unenforceable."

A number of submissions emphasized the distinction between confidentiality, as needed in business-to-business transactions and privacy as needed in transactions between clients and service providers, privacy being a relationship issue rather than a confidentiality issue. One individual response recommended that the right to privacy should not imply a right to anonymity and suggested that there should be no right to anonymity for mass e-mailers or those posting web pages on business or public matters.

Law enforcement issues

It will be noted from the quantitative responses that there appears to be a strong division of opinion between the law enforcement/national security interests and the rest of the respondents on the issue of control of cryptography. This is in part due to the fact that many of the law enforcement responses simply endorsed, without qualification, the August '97 resolution of the Canadian Association of Chiefs of Police (Annex A) which proposes, *inter alia*, establishment of a mandatory key recovery regime and legislation requiring real-time decryption for law enforcement access purposes. The parts of this resolution that propose mandatory, or additional controls on encryption have been strongly rejected by the vast majority of other respondents. On the other hand, some of the law enforcement responses reflect a recognition of both the challenges presented by cryptography and the need to find an acceptable solution that meets law enforcement needs without violating the rights of the individual. One law enforcement submission noted that, while the demands may appear to be an obstacle to progress, law enforcement is not looking for increased investigative capabilities or new authorities, merely to restore and maintain what was available before.

Overall, the submissions strongly support the statement made by one respondent that there is no popular consensus, outside the law enforcement community, that regulation of cryptography is needed. Forty-six submissions provided comments indicating that they believe no regulation of cryptography is needed and/or that existing methods available to law enforcement agencies to obtain information are sufficient to protect public safety and national security. These responses included 28 from individuals, 5 from carriers/associations, 5 from

privacy interests, 2 from industry associations and 6 from other groups. One carrier association noted that "the needs of users, carriers and third-party suppliers of E-commerce are in some cases in direct conflict with the stated needs of law enforcement and security agencies". A number of submissions, including one from a Privacy Commissioner, observed that the law enforcement agencies have not proven that the interception and decryption capabilities sought will lead to a decrease in criminal activities and it was clearly indicated that many respondents (46 submissions) believe that existing methods available to law enforcement agencies to obtain information are sufficient to continue to protect public safety and national security.

Although many of the submissions recognized the need to find a solution to the problems posed for law enforcement by strong cryptography, the impracticality of trying to control cryptography was repeatedly emphasized and there was virtually no support for mandatory key recovery or mandatory controls on carriers beyond the measures that currently exist.

While some of the demands made in the law enforcement submissions appear unlikely to find much support in the community at large (eg the requirement for registration of every Canadian citizen and landed immigrant in a key recovery system and the assignment of a unique password to all registrants) other police agency suggestions are more in tune with the bulk of submissions in that they recognize the technical difficulty, impracticality and cost implications of trying to apply mandatory access controls for stored data or mandatory access requirements on the carriers. Implicit in a small number of the law enforcement submissions is a recognition that the problem faced by law enforcement is not one of cryptography alone, but of the rapid pace of technological change and development of technical capabilities that can be abused. Comments that law enforcement agencies are not equipped to deal with current technology appeared in several contributions including a number from the law enforcement agencies themselves. It was suggested that additional tools, technical information, technical support, more resources to monitor and detect breaches, plus a national strategy are needed to keep abreast of the technology and to help technology fulfil the promise of aiding, rather than hindering, law enforcement.

Several proposals to meet law enforcement needs were made by groups other than the law enforcement agencies. These include: using court orders to gain access to keys; enforcing existing laws on surrender of information; gathering information by means other than examining encrypted files; cryptanalysis; and using existing and emerging techniques for gathering computer and non-computer data. One law enforcement submission recommended, as an alternative to mandatory controls, minimum standards to allow the federal government to provide education, direction and structure for cryptographic use and development. Another law enforcement response, recognizing the magnitude of the task of trying to apply encryption regulations, recommended that, "if the problem defeats all attempts at legislative control, alternative strategies and support for the development of investigative techniques be

pursued in parallel with existing initiatives". One industry association suggested the need for on-going dialogue between encryption producers, users and law enforcement agencies and offered to host such a dialogue.

The recommendation that use of cryptography in the commission of a crime be criminalized is included in the resolution of the Canadian Association of Police Chiefs and is frequently mentioned in the submissions from the law enforcement community. While there is no indication of strong support for this from the other submissions, it was also suggested by one of the industry associations.

Export Controls

Two issues come through very strongly here: Canada is being placed at a competitive disadvantage by the current application of export controls; and it is necessary to work in concert with the international community.

From the quantitative results, it can be seen that only 7% of respondents favour maintaining the status quo or extending export controls. In every group of respondents other than the law enforcement group, the majority favoured relaxation of controls. (Only four of the law enforcement submissions responded on the export control issue. One favoured extending controls, one favoured the status quo, one opted to remain neutral on the subject but to support any federal government initiative or decision, and one acknowledged there are some arguments in favour of relaxation but urged caution and noted the need to remain aligned with the US.)

Twenty-four submissions (including those of three industry associations, four carrier/associations and eight suppliers) included comments on the negative effects of current restrictions on the export of cryptography. The point that export controls put Canadian cryptography suppliers and producers at a competitive disadvantage was particularly emphasized. Many of those arguing for relaxation of export controls also emphasized the need to continue to work with the international community on this issue but, as several submissions observed, the Wassenaar provisions are being flexibly interpreted by some other countries. The example of the US giving blanket approvals to certain companies to export strong cryptography was given in considerable detail in one of the submissions. Germany, Switzerland and the Republic of Ireland were also mentioned as countries that allow companies to freely export cryptography products. It was noted that Canada fails to take advantage of this flexibility within the Wassenaar arrangement.

Although there is an overall clear preference for export controls to be eliminated, it was strongly suggested that, if export controls are to remain in effect, Canada should take maximum advantage of the flexibility under the Wassenaar arrangement to liberalize the controls to the greatest extent possible.

Two of the submissions argued that commercial crypto products should not be

subject to military technology controls noting that crypto products are important commercial tools and are now used more by business than by the military.

Suggested options for the export rules include giving blanket export approval for encryption up to a certain key length with case-by-case approvals for key lengths greater than that specified (128 bit keys for symmetric and 1024 bit keys for asymmetric encryption are recommended). Another suggestion is that export controls be abandoned except for specific embargos to individual countries. It is also suggested that both public domain and mass market software and hardware should be exempt from controls, that general approval be given to export a product, rather requiring individual licences for each export instance, and that Canadian exporters be permitted to match the product exports of other countries with products of similar strength.

The need for suppliers and carriers to be treated equally

Although mandatory controls and regulations are generally opposed, the point is frequently made that, any policy decisions must be technology-neutral and, if there are to be obligations placed upon suppliers, there must equal treatment for all.

In particular, three carriers/carrier associations urged that the application of assistance orders and obligations to cooperate with law enforcement agencies should apply to all carriers and service providers, not just those considered to be part of the public switched telephone service. One of the law enforcement submissions also noted the need for equal treatment for industry in the application of mandatory access and lawful interception. One submission commented that selective controls and licencing (such as licencing conditions imposed on wireless carriers) distort the market place and place an unfair burden on particular suppliers. As one submission observed: "As the telecommunications industry is becoming increasingly competitive, it would be inappropriate for the government to create a policy that distributes the burden of complying with policy directives in a manner that creates a competitive disadvantage for one type of service provider over another."

The carrier associations and two suppliers also recommended that any controls placed on the commercial use of encipherment should apply to all sectors of the economy.

The issue of equal treatment also came up with respect to export restrictions where one supplier urged that mass market and generally-available crypto hardware be given the same treatment as crypto software.

Legislation, regulation and Charter issues

Nineteen submissions (14 from academia, two from carriers/associations, two from privacy interests and one from a privacy commissioner) expressed concern that policy proposals for law enforcement and mandatory controls on real-time communications would violate the *Charter of Rights and Freedoms*, and/or laws including the *Telecommunications*

Act. Some of the law enforcement submissions noted that any potential legislation must be in accordance with the *Charter of Rights and Freedoms*. One of the law enforcement submissions suggested that arguments presented as to the *Charter* rights of Canadians to enjoy privacy and freedom of expression should be a "none issue" (sic) as any interception would require justification and the prior approval of the courts.

Liability issues were raised in five of the contributions, particularly the liability of third parties for the unauthorized release of confidential information, such as keys, and the liability issues that arise if companies are required to keep confidential information but are constrained by law to use only weak encryption or encryption with third party access.

One of the law enforcement responses noted that there is no specific authority in the *Criminal Code* that compels the possessor of a cryptographic key or a password to divulge the information. It was also noted in the same submission that recent *Criminal Code* amendments react to problems after they occur, which makes it difficult for law enforcement agencies to stay ahead of the technology.

A number of submissions urged that any action by the government should be proportionate to the extent and significance of the problem, and that account be taken of the probable cost of the response and the likely effect on both the targeted population (eg criminals) and everyone else (business and commerce, service providers, equipment and software providers, and users and the public at large). A number of individual and privacy/human rights submissions questioned the need to limit the privacy rights of all Canadians on the basis of assumptions and suppositions, devised by law enforcement and national security interests, when there is no real evidence that police investigations are being critically impaired by cryptography. An industry association pointed out any law enforcement and national security requirements that limit the application of strong cryptography would not only compromise the industry's security programs but might also have associated costs that offset the consumer benefits of electronic commerce. A number of submissions urged that a full cost benefit analysis be conducted before taking decisions on any proposals. Others recommended avoiding setting up a decryption/monitoring facility for all users when only a small number are targeted.

Submissions from the public sector/Privacy Commissioners stressed the need to ensure that the required encryption infrastructure is secure and trusted and also that cryptography policy binds trusted third parties to strict privacy principles and practices.

Other issues

A number of submissions pointed out that a strong case can be made that widespread use of strong encryption may advance effective law enforcement more than it may permit some individuals and organization to communicate privately about illegal acts.

Six submissions urged that cryptography policy and rules take full account of open, international standards. One industry association response referred to the patchwork of digital signature legislation in the US and said that standards are needed in Canada to avoid the same thing happening here.

One association pointed out the need for caution in using imported crypto products which could have undocumented features that allow third parties surreptitious access to a user's transactions. Some form of assessment and certification of crypto products was suggested.

A corporate submission urged that companies with a large customer base should be allowed to provide Certificate Authority services.

Conclusions and possible follow-on actions

A number of strong messages emerge from the comments and responses. It is clearly indicated by the majority of responses and the accompanying rationale that:

- mandatory controls on the use or importation of encryption facilities are unacceptable to business, industry, commerce, privacy and human rights advocates, academics and private individuals, as is any kind of mandatory key escrow/key recovery system;
- mandated access to decrypted real-time communications data can only be achieved at great cost and at significant risk to Canadian competitiveness and personal privacy;
- new measures to provide access to encrypted stored data are generally regarded as unjustified and unnecessary;
- current application of export controls is inconsistent internationally and is disadvantaging Canadian business;
- market-driven solutions are preferred to other alternatives for the listed policy options;
- law enforcement agencies face a significant challenge to some of their traditional investigative techniques from strong cryptography and other technological developments.
- there is serious concern that actions stemming from current policy proposals will have an adverse impact on personal privacy, and in particular, that law-abiding citizens will be disadvantaged by proposals to support law enforcement needs.

The following is a summary of possible actions suggested by the submissions to meet the needs of law enforcement agencies, business, industry, commerce, and the private citizen:

- federal legislation to make it an offence to use encryption to conceal criminal activity;
- changes to the *Criminal Code* to make it an offence to refuse to surrender an encryption key or to provide plaintext information in response to a court order;
- federal legislation to legitimize and recognize the use of digital signatures;
- federal legislation to protect the cryptography user against unauthorized release of his/her key, or other protected information, by third parties;
- assistance to the law enforcement agencies to enable them to keep abreast of technological change and to use the technology in a practical and realistic way to assist them in upholding the law;
- establishment of an on-going dialogue between law enforcement agencies, service providers, and cryptography and other hardware and software suppliers to assist law enforcement agencies in their task;
- progressive easing of export restrictions, consistent with Canada's Wassenaar obligations
- active encouragement of the legitimate use of strong cryptography as a way of building confidence in secure electronic commerce and electronic service delivery and as a way of reducing electronic crime.

Part 3: Suggestions for expediting the rollout of secure electronic commerce

Responses to the invitation to comment on measures to accelerate the rollout of secure electronic commerce were contained in a number of the submissions, though many of the respondents chose to confine their remarks to the cryptography policy issues. The suggestions below are drawn from the submissions that elected to comment on this issue.

Legal issues

1. Establish legislation that is formulated to provide a national framework that recognizes the validity of electronic authentication methods with the same standing as written signatures.

2. In facilitating the admissibility of computer-generated records for evidentiary purposes, ensure that laws facilitate the use of electronic methods (such as digital signatures), rather than imposing onerous and complicated regulatory schemes as has been done in some jurisdictions.
3. Foster an environment in which the market place, through national and international standardization schemes, is encouraged to develop the detailed procedures to underpin the reliability of authentication schemes.
4. Work to clarify the liability rules, particularly those associated with digital signatures and the unauthorized release of information by third parties.

Trusted Third Parties

1. Adopt a market-oriented approach to the establishment of Certification Authority services. A licencing regime at this point would be a burden on both the electronic commerce users and the emerging infrastructure. (Note that some existing institutions, such as the financial institutions, the Passport Office and the Post Office, appear well qualified to act as CAs.)
2. Recognize that the best way to achieve effective business practices for CAs, with minimum impact on cost and efficiency, is to encourage the private sector to develop CA procedures, in consultation with the public sector.

Lead by example

1. The government should play a leadership role as a model user of electronic commerce and electronic service delivery and also play a major role in the public promotion of these services and in educating consumers in their use.
2. The federal government should expand upon its role as a model Internet user and purveyor of on-line services, such as electronic tax filing, by accelerating and expanding the range of on-line services (for example electronic forms are not yet available via the Internet) and by enabling the citizen to interact directly with departments.

Security for electronic commerce

1. Recognize that cryptography is only one component in the security infrastructure that is essential for on-line government services. It is essential that information stored locally be securely held, be safe from intrusion and be recoverable in the event of failure or disaster.
2. The application of cryptographic products and services will have an enabling effect on all

sectors of economic and social activity. Without wide availability and deployment of encryption, the ability to create new, more competitive forms of business will be substantially inhibited. Strong cryptography is necessary to the success of electronic commerce and its use should be encouraged.

3. Ensure that any policies are based on open, international standards.
4. Ensure that protocols, software and encryption algorithms are well documented and freely available so that knowledgeable users can verify the strength and quality themselves. Avoid restrictions on the design, creation or implementation of strong cryptography.
5. Consider establishing, or recognizing, an independent assessment facility to provide users with assurance of the strength and reliability of cryptographic algorithms.

Role of government in promoting the electronic services

1. Consumers do not yet feel confident that the Internet is a safe way to transact business. The government needs to work with the private sector to develop effective security procedures and to educate the public about those procedures. Work to build consumer confidence.
2. Avoid over regulation, which will stifle technological development and hamper consumer confidence in electronic commerce.
3. Ensure that policies on cryptography do not unduly interfere with the ability of Canadians to protect the privacy and integrity of their electronic communications.
4. Avoid any measures that would unduly increase the cost of doing business electronically.
5. Support and actively assist the Canadian IT industry in providing security for electronic commerce.
6. Acquire and promote Canadian IT security products and services.
7. Encourage inter-operation of federal government security infrastructures (such as PKI) with the other public and private sector security infrastructures.
8. Allow the market place to work and ensure a level playing field for the Canadian IT security industry.
9. Work towards ensuring that everyone has access to on-line services, not just those who can afford their own computers and Internet services.
10. Avoid forcing people to purchase specific commercial software, or to go through

particular agents, as is now required for electronic tax filing.

11. Ensure costs of inter-operating with the government security infrastructures is low.

International issues

1. Continue to work in international fora to promote secure global electronic commerce and reduce barriers to global trade in cryptography products and services.

Closing remarks

The analysis provided in this report is, of necessity, limited to an overview of the most frequently occurring issues together with a subjective selection of some of the less frequently identified concerns. Although such analysis can provide an overview of the broad consensus, the richness of detail and the particular insights reflected in the individual responses cannot be captured except to a very limited extent. As mentioned earlier in this report, the individual submissions reflect a great deal of thought and effort on the part of the individuals and organizations who responded to the Industry Canada paper. These contributions provide a wealth of detail and much insight into the difficult task of developing a balanced Canadian policy on cryptography. Thanks are due to everyone who took the trouble to respond on this topic and who has in some way contributed to developing a consensus on this topic.

Annex A: Resolution of the Association of Canadian Chiefs of Police, August 1997

Therefore be it resolved that the Canadian Association of Chiefs of Police urges that the Government of Canada:

1. Establish a Public Key Infrastructure requiring licenced Certification Authorities and a mandatory key recovery regime which will provide for lawful access to cryptographic keys;
2. Enact appropriate legislation, including Criminal Code amendments to make the use of encryption in the commission of a any crime an offence and permitting the seizure of any equipment utilized for the purposes of encryption;
3. Enact appropriate legislation requiring that hte providers of encryption services to design such services to permit contemporaneous or real-time decryption for the purposes of lawful access by law enforcement and national security agencies;
4. Enact appropriate legislation to ensure that existing or emerging communications services manufacturers, services providers and network operators provide lawful access to communications at no cost to law enforcement agencies;
5. Establish an appropriate legislative and policy base to allow the Communications Security Establishment (CSE) to provide assistance to Canadian law enforcement and national security agencies in the area of cryptography and similar technology used in the commission of an offence;
6. Establish government standards to ensure confidence in information infrastructure which would reduce the potential of their use for criminal enterprise or other uses which are contrary to the public interest;
7. Increase the availability of resources to permit a higher level of research and development of technological and other measures to remove some of the obstacles to law enforcement and national security posed by cryptography and similar technology.

Annex B: Index of Submissions to the Discussion Paper

1) Summaries of Submissions from Organizations

Action Software International	042
Alliance of Manufacturers & Exporters Canada	1-314
Brockville Police	070
British Columbia Civil Liberties Association	139
Canada Post (Electronic Services)	1-302
Canada Post (Electronic Products and Services)	1-308
Canadian Advanced Technology Association (CATA)	125
Canadian Association of Internet Providers	123
Canadian Bankers Association (CBA)	118
Canadian Business Telecommunications Alliance (CBTA)	1-317
Canadian Cable Television Association (CCTA)	112
Canadian Security Intelligence Service	1-311
Canadian Wireless Telecommunications Association (CWTA)	166
Chrysalis-ITS	129
City of Charlestown Police Headquarters	063
Commission d'accès à l'information du Québec	094
Delta Police Department	160
DMR Consulting Group Inc.	037
Domus Software	126
EWA	168

Edmonton Police Service	171
Electronic Frontier	116
Entrust Technologies	130
Gandalf Graphics Limited	157
GT Group Telecom Inc.	031
H&R Block Canada Ltd. (Calgary)	163
Halifax Regional Municipality	169
Hewlett-Packard (Canada)Ltd. (Mississauga)	137
Information and Privacy Commissioner/Ontario (Ann Cavoukian)	128
Information Systems Manager Hyprotech Ltd. (Calgary)	156
Information Technology Association of Canada	153
Information Technology Laboratory National Institute of Standards and Technology	006
Institute for the Study of Privacy Issues (ISPI)	090
Intelligent Switched Systems	077
IT Management Consultant	013
KPMG	133
La Fédération nationale des associations de consommateurs du Québec et Option consommateurs	143
London Police	093
Manitoba Association for Access and Privacy	124
Metropolitan Toronto Police	142
Microcell Telecom Munciations Inc.	136

Mimosa Systems Inc.	146
MIT Lab for Computer Science	046
Motorola Canada Limited	141
Northern Lights College	045
Okiok Data Ltd.	099
Prince Albert Police Service	170
Privacy Commissioner of Canada	162
Queens University	101
Regina Police Service	167
Rogers Communications Inc.	152
Science, Research and Information Technology (Alberta)	127
Royal Canadian Mounted Police (Ottawa)	095
Royal Canadian Mounted Police (Ottawa)	097
Royal Canadian Mounted Police (Vanier, Ont.)	1-312
Royal Canadian Mounted Policy (Victoria, BC)	164
Royal Canadian Mounted Police (Whitehorse, Yukon)	115
Royal Newfoundland Constabulary	092
Stentor Telecom Policy Inc.	131
Telus Corporation	140
The London School of Economics and Political Science	135
Timestep Corporation	087
Twiggy Design	113
Université de Montréal	144

University of Toronto	039
University of Toronto (Department of Electrical and Computer Engineering)	138
Valmet Automation	108
Vancouver Webpages	081
Vidéotron Télécom ltée	1-318
Victoria Police Department	117
Ville de Québec Servie de police	159
Windsor Police Service	067
WinMagic Inc.	098
Winnipeg Police Service	047

2) Summaries of Submissions from Individuals

Arzumania, Ara	066
Bartel, Mark	056
Bernier, M.V.	058
Caldwell, Joshua	1-310
Chappel, David A.	1-313
Chin, Tony	052
Clayton, Michael J.	079
de Raadt, Theo	002
Darwin, Ian	132
Décarie, Richard	102
Duford, Lee	059

Galloway, Dave	154
Graham, Hugh	121
Gregory, Don W.	091
Harminc, Tony	1-300
Hart, Rob	085
Hayes, Amos	1-301
Hekimian, Hrad	066
Hinke, C.J.	1-315
James, Mark	100
Jeffery, Jim	027
Jeppsson, Jonas	119
Klassen, Arthur N.	078
Kossmann, William	054
Litwyn, Jay	015
Lloyde, William	032
Lynne, Stuart	053
MacGregor, John	060
Macrae, Robin	1-309
Maniscalco, Nick	109
Martin, C.	062
McCutcheon, Mark	151
McElvanney, Matthew	034
Milliken, Peter (House of Commons, Kingston)	172

Narveson, Jan	106
O'Malley, Sarah	155
Perrin, D.B.	040
Pick, Jim	089
Plumb, Marc	107
Quinton, Reg	075
Reid, Robert	103
Robinson, Ken	145
Sampson, Curt	076
Savard, John	104
Schuetz, Marko	110
Smith, Eric S.	1-316
Spencer, Henry	158
Streifling, Jeffrey	073
Tarrant, Keith	035
Tomlin, Gord	042
Taylor, M.	1-303
Tyler, Nicholas	064
Tyson, Al	033
Wilson, Brad	072