INFORMATION TO USERS

This manuscript has been reproduced from the microfilm master. UMI films the text directly from the original or copy submitted. Thus, some thesis and dissertation copies are in typewriter face, while others may be from any type of computer printer.

The quality of this reproduction is dependent upon the quality of the copy submitted. Broken or indistinct print, colored or poor quality illustrations and photographs, print bleedthrough, substandard margins, and improper alignment can adversely affect reproduction.

In the unlikely event that the author did not send UMI a complete manuscript and there are missing pages, these will be noted. Also, if unauthorized copyright material had to be removed, a note will indicate the deletion.

Oversize materials (e.g., maps, drawings, charts) are reproduced by sectioning the original, beginning at the upper left-hand corner and continuing from left to right in equal sections with small overlaps.

Photographs included in the original manuscript have been reproduced xerographically in this copy. Higher quality 6" x 9" black and white photographic prints are available for any photographs or illustrations appearing in this copy for an additional charge. Contact UMI directly to order.

**Bell & Howell Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600**

UMI[®]

**CRYPTOGRAPHY AND ELECTRONIC COMMERCE: THE ROLE OF THE
CANADIAN GOVERNMENT IN FACILITATING A DOMESTIC AND GLOBAL
ELECTRONIC MARKETPLACE**

**BY
CHRISTOPHER MICHAEL BLAIN**

**A THESIS SUBMITTED TO
THE FACULTY OF GRADUATE STUDIES AND RESEARCH
IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF**

**MASTER OF ARTS
LEGAL STUDIES**

**CARLETON UNIVERSITY
OTTAWA, ONTARIO
MAY 2000**

COPYRIGHT CHRISTOPHER M. BLAIN 2000

**National Library
of Canada**

**Acquisitions and
Bibliographic Services**

**395 Wellington Street
Ottawa ON K1A 0N4
Canada**

**Bibliothèque nationale
du Canada**

**Acquisitions et
services bibliographiques**

**395, rue Wellington
Ottawa ON K1A 0N4
Canada**

Your file Votre référence

Our file Notre référence

The author has granted a non-exclusive licence allowing the National Library of Canada to reproduce, loan, distribute or sell copies of this thesis in microform, paper or electronic formats.

The author retains ownership of the copyright in this thesis. Neither the thesis nor substantial extracts from it may be printed or otherwise reproduced without the author's permission.

L'auteur a accordé une licence non exclusive permettant à la Bibliothèque nationale du Canada de reproduire, prêter, distribuer ou vendre des copies de cette thèse sous la forme de microfiche/film, de reproduction sur papier ou sur format électronique.

L'auteur conserve la propriété du droit d'auteur qui protège cette thèse. Ni la thèse ni des extraits substantiels de celle-ci ne doivent être imprimés ou autrement reproduits sans son autorisation.

0-612-52340-3

Canada

**The undersigned recommend to the Faculty of Graduate Studies
and Research acceptance of the thesis**

**Cryptography and Electronic Commerce: The Role of the Canadian Government in
Facilitating a Domestic and Global Electronic Marketplace**

Submitted by

Christopher Michael Blain

**in partial fulfilment of the requirements for
the degree of Master of Arts**

Thesis Supervisor

Chair, Department of Law

**Carleton University
May 2000**

Abstract

The development of electronic commerce and the global information infrastructure is at a critical juncture. Today, most forms of information can be stored and processed electronically. This means a wide variety of information with varying economic values and privacy aspects will have to be secured. Cryptography plays an essential role in protecting electronic information against threats from a variety of potential attackers. While cryptography is not the only factor contributing to electronic security, it represents a significant means whereby information can be protected. In order to safeguard information and transactions on-line, national governments and international organizations must play a role in the development of this technology. Key escrowing technology, digital signature technology, certification authorities, and Public Key Infrastructures are all areas where governments can develop standards. These standards will help protect consumers, maintain democracy and sovereignty, and promote e-commerce in general.

Acknowledgments

I want to thank Professor Michael Mac Neil (supervisor) and Professor Paul Davidson for their academic support and input.

I would also like to thank the following people for their direct involvement:

To my Mom for her support. To my Dad, my life long editor. And to Cassandra for her patience, support, and guidance.

Table of Contents

ABSTRACT	iii
ACKNOWLEDGMENTS	iv
1. INTRODUCTION.....	1
1.1 PROMOTING A SECURE ELECTRONIC COMMERCE INFRASTRUCTURE	1
2. COMPETITIVENESS AND REGULATION IN THE GLOBAL ECONOMY	5
2.1 LAW AND ECONOMY	5
2.2 TRADITIONAL ROLES OF THE STATE	9
2.3 GLOBALIZATION AND FACILITATION	15
2.4 GLOBALIZED DEMOCRACY	19
2.5 THE NEED TO SET BASIC RULES FOR CRYPTOGRAPHY IN CANADA	23
3. CRYPTOGRAPHY TECHNOLOGY	31
3.1 THE DEVELOPMENT OF CRYPTOGRAPHY AND ITS USE IN ELECTRONIC COMMERCE ..	31
3.2 THE EMERGENCE OF A KEY RECOVERY SYSTEM	35
3.3 ASSESSMENT OF CURRENT LITERATURE	40
3.4 CANADA'S CRYPTOGRAPHY POLICY	51
3.5 ASSESSMENT OF CANADA'S CRYPTOGRAPHY POLICY	54
4. SECURITY IN TRANSACTIONS: LEGISLATED STANDARDS VS. INDUSTRY DEVELOPED STANDARDS	58
4.1 DIGITAL SIGNATURES	58
4.2 CERTIFICATION AUTHORITIES	67
4.3 PUBLIC KEY INFRASTRUCTURES	75
5. AN INTERNATIONAL PERSPECTIVE ON E-COMMERCE SECURITY	83
5.1 THE ROLE OF EXPORT CONTROLS	83
5.2 THE WASSENAAR ARRANGEMENT	86
5.3 THE UNITED STATES	89
5.4 THE UNITED KINGDOM	93
6. CONCLUSIONS	99
6.1 THE ROLE OF INTERNATIONAL ORGANIZATIONS	99
6.2 THE ROLE OF THE CANADIAN GOVERNMENT	102
APPENDIX	104
BIBLIOGRAPHY	109

1. INTRODUCTION

This introductory chapter identifies the policy issues and problems associated with the use of cryptography in electronic commerce. It sets out the framework for this essay, and it describes the general thrust of the argument being made throughout the course of this work; namely, that it is necessary international organizations along with domestic governments regulate the use of cryptography.

1.1 Promoting a Secure Electronic Commerce Infrastructure

The emergence of Cyberspace has brought about a new way of doing business. Some of these new techniques have the ability to become the most powerful tools in business. Commercial transactions, however, between individuals and businesses using Cyberspace raise a variety of issues about the adequacy of this medium for this purpose, particularly with respect to how capable they are of providing general transactional security. The lack of perceived security is a barrier to the growth of on-line commerce.

While cryptography is not the only factor contributing to electronic security, cryptography represents a significant technological means whereby security concerns can be addressed. As a result, cryptography is important to the growth of electronic commerce because it allows users to authenticate and safeguard sensitive data such as credit card numbers, personal e-mails, and other types of information. With an ever-increasing move towards the private development of cryptography technology and the implementation of public key infrastructures, as well as a move towards the need for some form of international standard in this area, the role of territorial governments remains unclear.

Heading into the twenty-first century Canada is faced with developing a national policy on cryptography in order to promote electronic commerce. In doing so it is necessary that the supporting infrastructure, including the procedures and physical components, be designed to ensure interoperability with other countries. The latest pronouncements on cryptography in electronic commerce from the Government of Canada indicate that it is adopting a hands-off approach with respect to regulation, although export controls are an exception to this. While the government is adopting a hands-off approach, it has at the same time assumed a 'model user' approach towards the use of cryptography.

The following is an attempt to ask whether or not this approach is an advantageous course of action. In doing so, it will ask whether or not the Canadian government should play a role in the development of cryptography. If so, it will then ask what role the Canadian government should play in the development of cryptography technology in order to ensure the growth of the Canadian electronic commerce sector?

On a micro level of comparative analysis this question reveals a tension between the market developing and regulating these technologies, and state regulation. Should the Canadian government pass legislation to provide minimum technological standards for Cyberspace transactions? Or, should the market set the standards for electronic commerce? In addressing this issue four specific areas will be researched; namely, key escrowing, digital signatures, certification authorities, and public key infrastructures.

Chapter 2 begins with a look at the role of law and government in the economy since the rise of the regulatory state. It establishes a framework for government intervention in cryptography technology, and illustrates the need for government

intervention. This chapter openly encourages the Canadian government to legislate minimum encryption standards in order to provide a higher degree of certainty in electronic commerce. It is also argued that this legislation will maintain democratic and sovereign control over Canada and its citizens.

Chapter 3 focuses on encryption technology and the controversial idea of key escrowing. Key escrowing systems are discussed in the context of security, consumer protection, and the general promotion of electronic commerce. In this chapter it is argued that key escrowing is not an area where the Canadian government should be setting minimum standards.

Chapter 4 takes a brief look at specific, yet important, components of cryptography in e-commerce; namely, digital signatures, the role of certification authorities, and the establishment of a public key infrastructure. Two perspectives are assessed for each of these technologies. Should the government set a minimum standard to ensure security? Or, should industry develop the necessary standards? It is established that digital signatures require legislation to ensure security. As well, the role of certification authorities should be mandated to ensure certainty in a public key environment. Moreover, it is argued that the 'model user' role the Canadian government is adopting through the Government of Canada Public Key Infrastructure (GOC PKI) is not sufficient.

Chapter 5 is a concise international survey of cryptography regulations. The intention of this chapter is to illustrate the trend to de-regulate the use of strong encrypted products in the United States and the United Kingdom. It is argued that this trend shows

the importance of encryption products internationally. Consequently, the requirement to use strong encryption should not be discounted.

When I started this research I believed that territorial governments would have to play a large role in developing cryptography standards partly because private industry would be incapable of protecting consumer interests. To some measure this is the conclusion of this work, however, I now believe that international organizations will play just as important a role as national governments. In the end, it is suggested that international organizations and national governments prescribe minimum standards for the use of cryptography in order for electronic commerce transactions to reasonably engender certainty and general consumer protection.

2. COMPETITIVENESS AND REGULATION IN THE GLOBAL ECONOMY

This chapter traces the role of government and law in a mixed economy. It will illustrate how our economy has changed, how the law has reacted, and suggest ways in which the law and government should react to contemporary cryptography. This section will begin with brief definitions of the state, mixed economy, and regulation. The analysis will begin with an historical look at traditional roles of government since the rise of the regulatory state. By looking at these traditional roles it is hoped that a framework for basic government intervention can be established. As well, the traditional roles of government will help illustrate the dramatic change our economy has undergone. Modern conceptions of the law and economy will then bring to light some of the roles of government in a globalized economy.

This analysis will provide a basis for the conclusions at the end of this chapter; namely, that the Canadian government may need to legislate in accordance with international model laws in order to provide minimum standards for cryptography because this domestic legislation will provide a higher degree of certainty that will allow electronic commerce to prosper. As well, the following chapter will encourage the Canadian government to take action because of the importance in maintaining sovereignty and democracy in this area. Analysis at the end of this chapter on globalized democracy will help illustrate this importance, even with an ever-increasing move towards globalized issues and solutions.

2.1 Law and Economy

Governments do a great deal that affects our daily lives. Governments can tax, spend, redistribute income, and they can regulate. They set the legal frameworks by which we

are governed, they regulate the services we consume, and they directly provide a vast array of goods and services. As pervasive as these actions may sound, few really appreciate the full range of what governments do. Fewer still understand how those activities affect the performance of the economy. In reality, however, it is important to Canadian society that governments be efficient and accountable. In fact, if Canada is to be competitive in international markets, it is essential.

Although one must recognize the importance of government, one must also realize that any legal order is a reflection of certain political and social values. In short, it is the political and economic factors themselves that determine what the government's role should be in the economy. Moreover, it must be recognized that two functions of law will strictly be confronted in assessing the role of government in the economy from a legal perspective.¹ The first function is the ability of law to impart some form of order to a system. For example, order can be imparted into a variety of political, economic or social phenomena. Second, the role of government can impart the function of the rule of law. In essence, government can provide some basis for justice and equality for the citizens, private industry, and the government itself.

There are many different ways of defining the state, the economy, and regulation. One brief example of different contemporary understandings of the state is between Hegel² and Marx³. The state for Hegel was one of necessity and the embodiment of individual freedom. In this conception, the state is not just an organization or a focus of

¹ W. Friedmann, *The State and the Rule of Law in a Mixed Economy* (London: Steven and Sons, 1971) at 10.

² See generally S. Avineri, *Hegel's Theory of the Modern State* (London: Cambridge U. P., 1972).

power, but the supreme embodiment of a person's individual and social aspirations. For Marx, however, the state is merely the administrative executive and legal machinery by which the ruling class ensures its control over the means of production and the exploitation of the working class. More to the point, for Marx the state is an instrument of oppression.

Between these extremes there are a number of philosophers that have tended towards either Hegel's version of the state, or Marx's version of the state. The following will use Wolfgang Friedmann's conception of the state as a focus of centralized power.⁴ This power is a result of the balance between various contending social and economic interests. Further, this power, according to Friedmann, is the embodiment of certain ideas of justice and public interests encompassing the community as a whole. The relevance of this definition in our modern and pluralistic society comes from the help the state may be invoked to offer either against private power (e.g.: price controls) or against public power (e.g.: judicial restraint).

The following also adopts Edward Mason's definition of mixed economy as a situation in which the role of government as owner and regulator has become sufficiently large to cast doubt on the validity of 'capitalist' and 'free enterprise' as appropriate adjectives, but not sufficiently large to justify the appellation 'socialist'.⁵ In doing so, countries and economies that have become totally socialized are excluded from this analysis partly because these countries rely on centrally directed planning as the major

³ See generally K. Marx, *Marx: Early Political Writings* (Cambridge: Cambridge University Press, 1994).

⁴ *Supra* note 1 at 2.

⁵ E. Mason, eds., *The Corporation in Modern Society* (Cambridge: Harvard U.P., 1960) at 15.

means of production. By contrast, the economies and countries that will be discussed in the following (e.g.: Canada, the United States, and the United Kingdom) are those where public and private enterprise to some measure still coexist.⁶ It is within these mixed economies that the power of the state is used to control or direct the economic system of the country, even insofar as it remains operated by private enterprise.

While the concept of the state and economy are important in the following, so too is the term regulation. Consequently, it is useful for analytical purposes to distinguish between government policy instruments. That is, to identify government actions that take the form of rules and controls directed at economic activities, with actions that are designed to provide goods and services directly to the public, along with those designed to control social and moral behavior. The definition of regulation adopted for the purpose of the following is the definition employed by the Economic Council of Canada in its studies of regulation; namely, “the imposition of constraints, backed by the authority of a government, that are intended to significantly modify economic behavior of the private sector”.⁷ Given that government backs the constraints, this means that non-compliance can lead to the imposition of penalties.

This definition of regulation contains three characteristics that differentiate regulation from other forms of government action. First, the emphasis with this definition is on economic behavior and not social or moral behavior. Second, this definition focuses on the importance – and effects of – producers, distributors, and

⁶ It is recognized that a major question is the extent to which a mixed economy still exists in these countries, especially in the Canadian context as the Federal government continues to divest itself of companies such as CN, Petro Canada, Air Canada, etc.

⁷ Economic Council of Canada, *Responsible Regulation: An Interim Report* (Ottawa: Supply and Services Canada, 1979) at 43.

consumers choices. More specifically, choice restrictions are designed for the protection of the consumer and society and are therefore an important aspect of economic regulation. Third, this definition assumes the imposition of rules supported by penalties. These penalties may take the form of fines, loss of licence, or in the most severe case, jail terms.⁸

2.2 Traditional Roles of the State

From a Canadian perspective Allan Greer and Ian Radforth have argued that the rise of the traditional 'regulatory' state emerged in the mid-nineteenth century.⁹ They maintain that we see the expansion of government during the Union period. New departments were created, functionaries became more numerous and more professional, and budgets grew. Moreover, it is at this time that government took over a host of new responsibilities, most importantly in the area of education. To a considerable extent, Friedmann has summed up the traditional roles of the state in the economy since the rise of the 'expanded' state.¹⁰ Although Friedmann's analysis is mainly a comment on the economic, political, and social conditions of the 1960s, the four major roles of the state he identifies serves as an introduction to the possible roles the state can play in the economy, and will therefore be canvassed. Moreover, although the Canadian government has privatized and de-regulated to a considerable extent, *prima facie* Friedmann's analysis illustrates the changing discourse between the state and the economy. In the end, although the government is moving away from some of the roles Friedmann identifies,

⁸ John C Strick, *The Economics of Government Regulation: Theory and Canadian Practice* (Toronto: Thompson Educational Inc., 1990) at 3-4.

⁹ See generally Allan Greer & Ian Radforth, *Colonial Leviathan: State Formation in Mid-Nineteenth-Century Canada* (Toronto: University of Toronto Press, 1992).

¹⁰ See generally *Supra* note 1.

understanding these roles may be of some use in understanding the development of e-commerce.

The first function Friedmann identifies is commonly associated with the social welfare state, that is, the state acting as a provider. Within this capacity, the state ensures a minimum standard of living by making itself responsible for the distribution of certain social services. The state charges itself with this responsibility partly in the alleviation of the free play of economic forces (e.g.: although private insurance is available it is only received with the payment of premiums). The implementation of the ideal of the social welfare state is done in the most direct manner. Most often, benefits are directed through compulsory transfers on behalf of the community. This is done by various legislative and administrative procedures.

The scope and extent of the state's function as provider was potentially unrestricted. To some measure, unemployment insurance, sickness insurance, old age pension, and death benefits were among a solid core of the non-socialist welfare state provisions. Furthermore, in the distribution of these and other benefits, the state, by the use or non-use of its legislative and executive powers, was ultimately responsible for the intensity, and standards set for the various economic benefits.

This function later expanded partly because of the realization that in our modern industrial society individuals are exposed to a variety of risks over which they do not necessarily have control. Consequently, under an expanded function of the state as provider, it was not uncommon for government to set standards for automobile and air traffic, nuclear explosions, water pollution, safety of food and other mass-manufactured products, and for the use of pesticides – to name only a few. The assumption by the state

of an ever-widening range of social responsibilities continued to have a fairly large impact upon individuals for a number of decades. In fact, as Friedmann concludes, the ever-widening social responsibility of governments was a “necessary corollary of the social condition of man [sic]”.¹¹

Acting as a regulator, the state used various levers for control. Notably, the state had the power to regulate investment in industrial development and the volume and kind of imports and exports through means such as exchange controls and various industrial licensing controls. These devices are particularly useful for developing countries that suffer from more than a temporary balance of payments deficit and a foreign exchange shortage. In short, under the guise of regulator, the state interferes through the use of public law, making it seem as though it is still an unregulated society.

The available legal devices by which the modern state controlled activities of the community were almost immeasurable. Nevertheless, Friedmann compiled the most representative types of legal controls available under the following categories; legal restraints on freedom of contract and property, legal controls seeking to mitigate undue concentration of economic power, and legal controls directed to protect the national economy. Although even a highly selective and general survey of these regulatory devices is outside the scope of this work, one can easily imagine the complexity of these functions in the modern state with a mixed economy. As Friedmann suggested, the proliferation of these controls is due to the fact that “no modern society can watch

¹¹ *Supra* note 1 at 30.

passively the free play of economic forces".¹² In many cases, regulatory functions are the alternative to a full-scale socialized state. As a result many modern states have a multifaceted apparatus that consists of administrative agencies, quasi-judicial institutions, and even new branches of law, that in the end help straddle public and private law. Regulatory functions, therefore, had become to some measure indispensable – the question that often needed to be addressed was: are these functions sufficient?

Despite the indispensability of the regulatory functions the state could administer, the modern state had increasingly functioned in a more important role as entrepreneur. It is under this function that the state began to operate in various sectors of the economy by taking control either through semi-autonomous government departments, or through state owned corporations. As the function of entrepreneur presupposes the state acts both in the private and public sectors, certain fundamental issues were raised – most notably in the area of equality of treatment. Nevertheless, state enterprise continued to be a worldwide phenomenon. For example, in the United States, the Tennessee Valley Authority or the Boulder Dam Authority controlled an important part of the nation's power generation and distribution.¹³ Further, in various states a number of public authorities operated bridges, ports, waterways, and other public utilities.

Although there are various reasons for the growth of the state as entrepreneur, one main reason that can account for a great deal is that certain functions were regarded as vital for the nation as a whole. In essence, it was believed that certain economic activities were so vital to the survival of the nation that they could not be left to the private sector –

¹² *Ibid.* at 50. It may be recognized that there has been recent retrenchment from this view; however, it has not been to the extent that government feels as though they have no role in the economy.

partly because they could not be assured by the private sector. (Noteworthy examples have been the railways in vast states such as Australia and Canada¹⁴) Moreover, the need for a planned economic development within states led to the proliferation of entrepreneurship by the state. In short, a national economic development plan facilitated by state ownership designed to finance became attractive (most often in association with local capital or foreign investors).

The development of the state as entrepreneur is in direct conflict with the fourth function of the state – the state as umpire. Acting as a repository of legislative, administrative, and judicial power, the state was responsible for dispensing a standard of justice. Therefore, not only did the state have to enforce the rule of law between various private sector businesses, but it also enforced the rule of law towards businesses that were owned by the state itself. Understandably, one of the toughest tasks for the state was to differentiate between the entrepreneurial and the arbitral function that it should be performing.

Under a liberal conception of the state, the spheres of public and private activity are neatly separated. Government is precluded from actively getting involved in economic matters. Its principal functions are mainly to provide order, defence, policing, and the administration of justice. Nevertheless, as provider of social services, as controller of economic activities, and as entrepreneur, the government by the late 1960s had undoubtedly entered into the economic arena. Of the utmost importance at the time was that the state had standards and institutions that ensured minimum fairness. Moreover, the state provided and maintained a reasonable balance between the different

¹³ *Ibid.* at 52.

economic and social groups in the community. These activities were initiated partly because it was believed that, even in a totalitarian society, no basic philosophical principle of justice demanded an 'untouchable' sphere of autonomy for any group or individual.¹⁵ The implication was that, even in a mixed economy (where public and private sectors coexist) each had to have its legitimate sphere, and the function of the law was to ensure that both had a fair chance to operate. More to the point, law was to ensure that one sector would not strangle the other.

These conceptions of the mixed economy are evidently outdated – partly due to the new global economy and the government's changing role in this new economy. On the one hand, Friedmann's analysis acts as a reminder that the role of the state is not a fixed one. On the other hand, however, the governments' move towards privatization and deregulation confirms the realization that the state's role in today's economy may be very different than those identified by Friedmann. For example, the move towards the privatization of utilities illustrates the state's decreasing role as entrepreneur. Further, although the state to some measure still acts as a regulator, free trade has reduced certain kinds of controls on trade. Even certain economic benefits the state has provided have, over the past 5 to 10 years, been restricted. Nevertheless, despite the move away from these state functions, there are certain vital responsibilities the state may provide according to Friedmann's analysis.

In the ever-expanding world of Cyberspace technology the state could provide standards. With developments being made in both the electronic delivery and electronic service industry, the government is now in a position to become a leader and introduce

¹⁴ *Ibid.* at 54.

new ways of doing business on-line. Essentially, the government has the ability to create models for on-line transactions. In short, acting as a provider in our modern economy, and our modern technological field of electronic commerce, the government has the ability to substantially provide for citizens and at the same time deal with problems attendant with such technology; namely, privacy and security.

As well, the state function of regulator continues to a lesser degree to be an important function in our modern society. Even though recent pronouncements have been towards de-regulation of the Canadian economy, the function of regulator should not be totally dissolved in the global economy. This realization is especially evident once again in the electronic commerce field. Although the government is in a position to act as a provider (e.g.: provide minimum standards for encryption) it also must realize the importance of enforcing standards. In short, it is the government's duty, as regulator, to dispense the necessary justice and redress that should go along with standards.

2.3 Globalization and Facilitation

It is difficult to suggest that any one of the traditional roles of the state in the economy has had a more profound impact than any other because of the complexity of the relationship between the state and the economy. In today's changed economy, this complexity has increased. The need to negotiate new rules is based upon the fact that our economy has greatly changed – changed in the sense that the state has evolved and is no longer simply concerned with its own economy, but rather, its economy in the global village. As a result, one can no longer rely solely on the work of Friedmann because of this changed economy. In reality, therefore, the role of government in the economy starts

¹⁵ *Ibid.* at 71.

with the recognition of the tremendous changes that have taken place over the past few decades, which have left us with a new globalized economy.

The term globalization is used to identify the rapid and pervasive diffusion around the globe of production, consumption and investment of goods, services, capital and technology.¹⁶ The realization of the global economy is partly due to new developments in communications technology, transportation facilities, and a fundamental change in production¹⁷. In essence, these changes have led to a deep-seated transformation in the nature of the international economy. No longer are there simply exchanges among a set of inter-linked nations, but there are now exchanges within an integrated global economy.

To a considerable extent the computer chip has allowed for these transformations to take place. In fact, some have now begun to recognize the computer chip as being as important an invention as the printing press and the steam engine. In terms of our economy, the computer chip has given businesses the ability to gather, analyze, and store information at a level never experienced before. The magnitude of its impact some have suggested is even more far reaching. In fact, Michael Hart has suggested that some of the experiences within the last decade (low productivity and employment growth) are not due to depressions or business adjustments, but rather, are due to the slow responses of governments and institutions to the demands of the computer chip.¹⁸

In response to this development, businesses have revolutionized. Firms are now relying on smaller inventories, more synergistic links in the production chain, and a

¹⁶ Michael Hart, "What's Next: Negotiating Rules for a Global Economy" Occasional Papers in International Trade Law and Policy, No. 36 (Ottawa: Centre for Trade Policy and Law, 1995) at 2.

¹⁷ In the sense that the bulk of goods traded internationally are now parts and components for assembly into end products closer to the final point of consumption. *Ibid.* at 3.

greater emphasis on quality, not quantity.¹⁹ Moreover, with the development of the Internet, and the ability to transact on-line instantaneously with consumers around the world, we see the development of much faster business organizations based on the elimination of a huge army of clerks and middle managers. More to the point, globalization has developed a process that has become increasingly less bound by the limitations of time, space, and resources.

Businesses have also become less concerned with investing in geographical markets. In essence, international firms a decade ago would penetrate markets by investing in the local market. This would be accomplished by setting up smaller businesses within each local market that would produce a wide range of products for a geographically specific area. Today's global firms, however, are deliberately decentralized. Often, they locate several parts of the production process in various parts of the world according to both supply (access to labour) and demand (access to markets).

Although the foregoing is by no means an exhaustive analysis of reasons for our changing economy, globalization has accounted for wholesale changes in the pattern of international trade and investment. Consequently, it must be recognized that what is required are wholesale changes and adjustments to be made within and between national economies. As Hart comments, these changes in the economy have shattered the confidence of the generation that grew up under the four different roles of government that Friedmann identified.

Conditioned by a century of increasing government involvement in the economy, many are looking to government for answers and relief or blaming governments

¹⁸ *Ibid.* at 4.

¹⁹ *Ibid.* at 4.

for permitting these developments to take place. Governments, however, are as yet unprepared to address the full implications of managing a global economy. They have yet to recognize that we have reached the stage at which the kind of tradeoffs that were traditionally made at the national level, such as between efficiency and equity or producer and consumer interests, can now more effectively and efficiently be made at a super-national level – regionally and globally.²⁰

We have reached a point in our global economy where activity is increasingly influenced by extra-national transactions – for example, few goods, services, capital and technology are still produced wholly within a national boundary. To some measure, the previous regulatory structures that were built over the last few decades are now serving as an impediment, rather than a facilitator for economic growth (partly because they were based on the fact that economic transactions were taking place within the confines of the nation).

While some might decry the involvement of the government in the economy, few would seek a return to the *laissez-faire* conditions that had prevailed in the early part of the 19th century. This is especially true in western democracies as the regulations and institutions that were implemented were designed to supplement the market or stand in its place when the market failed to deliver socially or politically important objectives.²¹ In short, modern societies are taking for granted the effects government can have, and have had, that, in our new globalized economy, are counter-productive.

The challenge, Hart argues, is to find a way to recapture democratic control over the market, but in a manner geared to the reality of a global economy rather than a group of interlinked national economies. Hart implies that governments are as yet unprepared

²⁰ *Ibid.* at 5-6.

to handle this change partly because of their reluctance to marry the concepts of a globalized economy with the continued ability and desire of domestic governments to exercise democratic control over the operation of the market. More to the point, what is needed is a revolutionary set of rules that recognizes the needs of each state to exercise democratic control, and business needs to survive in the global economy.

2.4 Globalized Democracy

In the wake of globalization, the liberal democratic state to a large extent has begun to erode. As David Held and Anthony McGrew suggest, there are four major disjunctures that have helped separate democracy from the liberal democratic state since the rise of globalization.²² First is the continuing influence of global forces on the international security structures of a nation state. One of the essential functions of the democratic state is to ensure the security of its citizens and its own territorial integrity. As Held and McGrew articulate, however, a continued form of 'power politics' imposes significant constraints upon the kinds of defence and foreign policies which democratically elected governments may pursue. In short, there is an obvious disjuncture between a state's own notion of itself as an autonomous actor with independent military capabilities, and its insertion into a global power hierarchy of states and security structures that can impose their own actions or policies.

The second major disjuncture is the internationalization of the liberal democratic state. Held and McGrew imply that since the end of the cold war, states are increasingly engaged in multilateral forms of international governance. States now seem to be

²¹ *Ibid.* at 6.

²² David Held and Anthony McGrew, "Globalization and the Liberal Democratic State" (1994) 28 *Government and Opposition* 261 at 266.

involved in an expanding array of international organizations established to manage specific global issues (e.g.: oceans, space, telecommunications, trade). The increased participation of the state at this level has led to important developments in the structure of decision-making both in world politics and domestic politics. Although the state continues to at least theoretically maintain sovereign power, any conception of sovereignty that assumes it is an indivisible and exclusive form of public power is defunct. The continued internationalization of the state presupposes a number of external forces that can affect the sovereignty of any state.

The third disjuncture is the development of international law that has subjected individuals, governments and non-governmental organizations to new systems of legal regulation. Two specific regulations have curbed the rights and duties of democratically established states; namely, immunity from jurisdiction, and immunity from state agencies.²³ While institutions with coercive power or enforcement may not back them, Held and McGrew suggest that they nonetheless have far-reaching consequences. Ultimately, at the heart of this development is a conflict between the claims made on behalf of the states system, and those made on behalf of an alternative organizing principle of world power.

The final disjuncture is a result of the growth of a world economy. This disjuncture occurs between the formal authority of the state and the spatial reach of contemporary systems of production, distribution, and exchange, factors which, seem to

²³ The former stipulates that no state can be sued in the courts of another state for acts performed in its sovereign capacity. The latter specifies that should an individual break the law of another state while acting as an agent for his or her country of origin and be brought before that state's court, they are not guilty because they did not act as a private individual but as the representative of the state. *Ibid.* at 273.

limit the competence and effectiveness of national economic policies. They are particularly influenced by the production and the globalization of financial transactions. Further, national policies are influenced by the globalization of banking and financial services. These financial services are now operated by information technology that has helped transform the finance sector such that a single global financial market now exists with almost round-the-clock trading.²⁴

Before these four major disjunctures developed it is interesting to note that within the world's major regions there had been consolidation to democratic processes and procedures. In the mid 1970s more than two thirds of all states were authoritarian. Three decades later, that percentage has fallen dramatically; less than a third of all states are now authoritarian.²⁵ More to the point, democracy in the current era has become the fundamental standard of political legitimacy. Yet, at the same time regional and global pressures and problems increasingly challenge these very democratic principles. Taken together, the four major disjunctures articulated by Held and McGrew identify new patterns of powers and constraints that are redefining the architecture of sovereign democratic nation states.

Increasingly, questions and problems are being raised that require, to a large extent, global consensus. Some of these problems include the spread of AIDS, the flow of financial resources, the drug trade, international crime, and more recently, questions about the regulation of the Internet. Although addressing these questions is important, they have also brought about the colossal problem of how one would go about solving these problems within the democratic sphere. What kind of accountability and control

²⁴ *Ibid.* at 268.

can citizens of a single nation state have over international actors and actions? Can democracy be sustained in addressing these global issues? How can citizens participate as citizens in a new internationally organized world? In short, in addressing these questions, can democracy as we know it survive?²⁶

The purpose of raising these questions about globalized democracy is not to suggest ways in which we can obtain global democracy. Rather, the purpose of the foregoing is to suggest that democracy and sovereignty in the globalized world should be taken seriously. It is suggested that democracy and sovereignty are important concepts to foster, and that addressing global concerns at the national level is still important. To some measure, international model laws will continue to be the framework for domestic law, especially with regards to international trade and development. It is clearly recognized, therefore, that international model laws and conventions in the area of electronic commerce will play a significant role in Canada's domestic legislation partly because if they do not Canada risks creating trade barriers. To this end, Canada must remain active at the international level in order to properly represent Canadian interests. However, this does not mean that domestic governments are obsolete.

Democracy and national uniformity within Canada regarding electronic commerce will have limitations. This realization is certainly acknowledged as all domestic rules, both federal and provincial, will have to conform to international model laws if Canada wants to remain part of the global marketplace. Nevertheless, while the purpose of the foregoing was to bring more attention to democracy, preserving national sovereignty is a deeper concern raised with regard to electronic commerce and global

²⁵ David Held, "Democracy and Globalization" (1997) 3 Global Governance 251 at 251.

regulation. In short, maintaining national sovereignty will help prevent the exploitation of citizens in Cyberspace. Consequently, the challenge set is to find a way to recapture democratic and sovereign control over the market, but in a manner geared to the reality of a global economy.

2.5 The Need to Set Basic Rules for Cryptography in Canada

The market system allows competitive sellers to have access to a large number of consumers, whereby each consumer unknowingly promotes the public interest by striving for their own personal gain. This ideology has become so woven into our society since Adam Smith first remarked on this type of system back in 1776, that most economies that followed this path have achieved materially prosperous and technologically powerful economies.²⁷ In essence, the view most of these nations took was that the best thing the government could do for the economy was to leave it alone.

The belief in free trade, an aversion to all forms of price controls, freedom of occupation, freedom of domicile, and freedom of enterprise, are all corollaries to this system. Although these beliefs have become to some measure a background assumption for thinking about the relationship between the government and the economy, it would be misleading to think that these were the only factors that strengthened the world's most powerful economies. In essence, although there is a compelling argument to be made about the impact this type of system has had, there have been continuing roles of government that have helped guide the economy.

²⁶ *Ibid.* at 251.

²⁷ M. Froomkin & B. DeLong, "Speculative Microeconomics for Tomorrow's Economy" (1999), online: University of Miami Law School <<http://personal.law.miami.edu/~froomkin/articles/spec.htm>> (last modified: November 1999).

As Friedman has demonstrated, there have been a number of roles the government has played in the economy since the rise of the regulatory state. To suggest that modern states have not been prosperous because of government intervention since that time would be false. Rather, the government's involvement in providing the necessary infrastructures, the regulatory frameworks, and establishing and applying the rule of law, have all been important contributors to creating functional and prosperous economies.

As Hart has established, the various roles the government has played over the past few decades have changed dramatically. In short, as economies have changed and new technologies have affected the way people do business, the government has continued to evolve and change its roles and policies. Nevertheless, throughout all of these eras, the government has remained to a large extent a major contributor to the economy by setting regulatory frameworks and dispensing the rule of law.

The new globalized economy of Cyberspace should be seen as another area where the government will need to actively provide the necessary infrastructures and regulatory frameworks in order to facilitate the expansion of this new economy. Although consumers must have access to a large number of competitive sellers, and sellers must have access to a large number of consumers, there continues to be a role for government in this type of economy. This is so because electronic commerce will bring about a variety of new problems (e.g.: problems with regard to the authentication of documents, identities, etc.) that will require the law to recognize non-paper based agreements and transactions. In this regard, technological standards will be necessary to provide a solid foundation for the market system.

Protecting consumer interests on-line is a fundamental reason why government needs to establish a foundation for the market system. If Canada's success in the 21st century depends increasingly on the ability of all Canadians to participate and succeed in the global knowledge-based economy, then Canadians must be assured that transactions on-line will be authentic, and that their identity will be protected. In doing so, cryptography technology is available that will help supply this protection.

This technology will help protect against information being obtained by people for whom it is not intended. Consequently, cryptography technology will not help protect against companies compiling a detailed record of consumers' personal history and preferences. Accordingly, it is recognized that the consumer protection policy issues that cryptography raises are only a subset of the larger regulatory agenda relating to consumer protection and privacy. Nevertheless, cryptography is essential in electronic commerce because it can provide authentication, establish identities, and it can provide general transactional security.

The issue of security strikes directly to the heart of electronic commerce. While it has become increasingly important for the Canadian economy to foster this revolutionary technology, it has also become important to protect consumers on-line. In essence, in order to develop an electronic commerce industry, it has become increasingly well understood that no matter how or where consumers complete their transactions, personal data must, first and foremost, be protected from those for whom it is not intended.

There are several options by which transactional security may be achieved in Cyberspace. One is to have government regulated standards that prescribe a minimum level of transactional security. The second is to allow users to decide what level of

protection they wish to use. While there has been recent support for the latter²⁸, if the Canadian government were to leave the implementation of encryption procedures to private industry there is potential for severe consequences.

The protection of consumers' identities and personal data on-line may be compromised because of the advance in technology. Today, there exists technology that makes brute-force attacks against cryptographic systems once considered adequate, both fast and cheap.²⁹ Threats to the confidentiality of information come from a number of directions and their forms depend on the resources of the attackers. Hackers can be anything from high school students to commercial programmers who have access to mainframe computers or networks of workstations. With a relatively small budget these people can buy off-the-shelf chips that help increase the effectiveness of decoding encryption.³⁰ It was only 10 years ago that 56-bit encryption algorithms were unable to be decoded. However, today, these algorithms can be decoded in 22 hours.³¹ These advancements require government involvement to establish an on-going 'safe' level of cryptography software. In short, the government's role would be to set a minimum standard that would reasonably engender a high degree of confidence in electronic documents and signatures.

²⁸ See generally the Honorable John Manley's (Minister of Industry) speech on October 1, 1998, online: Task Force on Electronic Commerce <<http://e-com.ic.gc.ca/english/speeches/42d3.htm>> (last accessed: 11 March 2000).

²⁹ Matt Blaze et al., "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security" (1996), online: Counterpane Internet Security Inc. <<http://www.counterpane.com/keylength.html>> (last accessed: 3 April 2000).

³⁰ *Ibid.*

³¹ It was report by The Electronic Frontier Foundation (EFF) that it had broken 56-bit encryption in 22 hours and 15 minutes – a world record thus far. The EFF web page URL is: <<http://www.eff.com/>>.

If private industry set the standards in these areas, they would essentially be setting the requirements necessary for legal transactions. In essence, industry would be establishing the level of certainty required to establish that documents were signed, notarized, or under seal. In this case, if cryptography software packages were not used with an appropriate level of security, vendors and consumers would be at risk (e.g.: transactions may be vulnerable) and the entire electronic commerce infrastructure would be unstable.

The inability of industry to consistently update software to provide adequate protection to consumers stems from the fact that this technology rapidly changes, and as a result systems will have to be constantly updated. Over time, the sheer cost of updating this software and technology may be something that private industry will not do. This may be especially true of smaller firms on-line who may determine that a particular year's on-line sales margin does not necessary demand a new security system. As a result, the company may allow on-line security to fade, and put not only themselves, but also their customers at risk.

As well, the lack of consumer knowledge about data security leaves consumers vulnerable. In the short term, consumers will need the government to establish a security standard partly because most Internet users are still unfamiliar with cryptography and its applications. This inability to comprehend the functions and capabilities of encryption, and the levels of encryption protection, may leave many consumers with a false sense of security in that some may believe that all encrypted data is unintelligible without the necessary private key (e.g.: that encrypted data cannot be 'hacked').

In the long term, regulation will be justified because of market imperfections. If private regulation is adopted, industry can impose external costs on consumers partly because consumers may not be educated about the latest developments in cryptography (e.g.: consumers may be unaware when certain levels of encryption are deemed un-secure). Without minimum standards certain firms may not want to, or may not have adequate resources or the knowledge to update systems when they are deemed un-secure, thus leaving the consumer at risk. Regulation, however, would force the internalization of these costs by consumers. Consequently, setting minimum standards will ensure consumer and transactional security.

In addition, government intervention will be necessary to protect consumers because of the importance and potential magnitude of electronic commerce. As businesses globalize, and as computers allow for the transmission of data and communication worldwide, electronic transactions may become a vital component of Canada's economy. As on-line transactions are already under attack, the need for uniform security in the future will be necessary. Therefore, all transactions that take place on-line must be regulated in the sense that consumers must be assured that no matter with whom they do business, or how they do business; a minimum level of security will be met.

Although transactions currently take place via the Internet, a secure base set of minimum standards has yet to be formed. If governments legislate a minimum level of encryption it would provide a firm basis for legal standards upon which enforcement mechanisms could be established. More to the point, if international treaties and domestic legislation mandated a minimum level of encryption for e-commerce

transactions, certain public key cryptography, digital signature, and certificate initiatives may provide the certainty function served by written and signed documents today. In the end, this will help promote the electronic commerce sector within Canada.

If we accept that rule making is in our collective interest, we must pursue new directives. In short, governing bodies need to set standards – standards that reflect the emergence of a globalized and information driven economy. Realizing that a great many of these new transactions will occur via the Internet, it is imperative that governments (locally, nationally and internationally) take some steps in setting standards. To this end, domestic governments must realize their continued role as regulator in our new global economy because democracy and sovereignty must not be forgotten in creating and directing the domestic economy in this area – in large part because of the potential impact electronic commerce may have on citizens.

It must be recognized that although there will eventually have to be some form of global consensus, domestic governments still have a large role in the implementation of encryption standards. Liberal democratic states, therefore, need to consult with their citizens and reach a secure protocol for the implementation of encryption technology that can be universally used within their own nation, while at the same time recognizing international agreements.

Although regulation and government intervention may be necessary for a variety of encryption technologies, it must also be cautioned that severe government intervention in such a fast paced technological field may be counter-productive. With this in mind, the challenge is to identify one single component of encryption technology that may pinpoint the essence of transactional security – a component that governments (nationally

and internationally) could regulate without distorting innovation, and at the same time provide and ensure secure e-commerce standards. In regulating any component, it is clear that consumer interests, democracy, sovereignty, and the promotion of electronic commerce in general, must be kept in mind as new policies are shaped.

3. CRYPTOGRAPHY TECHNOLOGY

This chapter canvasses the development of cryptography to illustrate its usefulness in electronic commerce. As well, controversial key escrowing systems are discussed partly because escrowing keys is a common practice often associated with the use of strong encryption. Key escrow raises questions and concerns about both crime and civil liberties, and about electronic commerce; namely, concerns about security, consumer protection, and the promotion of electronic commerce as a whole. Much of the relevant literature on this matter will be analyzed as well.

In parts 4 and 5 of this chapter, Canada's cryptography policy as of October 1998 will be described and assessed in relation to the academic literature. It will be argued that although legislating mandatory key escrowing systems is unattractive and will ultimately create disincentives for electronic commerce users and businesses, legislating a mandatory minimum key length (e.g.: 128 bit or higher) is attractive.

3.1 The Development of Cryptography and its use in Electronic Commerce

Cryptography technology is as old as written language. The word cryptography is derived from Greek roots meaning "hidden word", and is used to describe the ancient science of secret communications. Until recently, this technology was mainly used by the government to safeguard military and diplomatic communications. Today, cryptography is an important component of secure information and communications systems (e.g.: digital electronic payment systems and telecommunication systems) and an essential technology for enabling electronic commerce.

A variety of applications have been developed that incorporate cryptographic methods to provide data security. Cryptography is a tool for achieving two related, but

distinct, aspects of data security. First, cryptography makes it possible to verify the integrity of data and/or the authentication of the sender of a message (using a “digital signature” function). Second, it provides a way of ensuring the confidentiality of data (using an “encryption” function).

As RSA Data Security Inc. suggests cryptography today might be summed up as the study of techniques and applications that depend on the existence of difficult problems.³² In short, these difficult problems are concerned with keeping communications private and secure by providing mechanisms such as digital authentication, data integrity, and confidentiality. The field of cryptography encompasses other uses, as well, that directly relate to the implementation of a secure electronic commerce infrastructure. With just a few basic cryptographic tools, it is possible to build elaborate schemes and protocols that allow consumers to pay using electronic money, or, to even prove that they know certain information without revealing the information itself.³³

Today, cryptography technology plays a large role in Internet security. While encryption is simply the use of some means to disguise or obscure the meaning of a message, transposing or substituting the characters that make up the message normally achieves this. Encryption is accomplished by a method prearranged by the sender and

³² RSA Laboratories, *RSA Laboratories Frequently Ask Questions* (1996), online: RSA Laboratories <<http://www.rsa.com/rsalabs/>> (date accessed: 11 March 2000).

³³ *Ibid.*

recipient so that only the intended recipient, who alone possesses the key to unraveling its true meaning, can read the message.³⁴

Contemporary cryptographic systems have two distinct mathematical families which both change one group of readable symbols into a second set of unreadable symbols by passing it through a complex mathematical process controlled by a number called a key. The secret key system (symmetric cryptographic system) uses the same number to do both encryption and decryption, allowing the encryption key to be calculated from the decryption key, and vice versa. (Partly because of the advancements in encryption techniques, even the fastest super-computer would take billions of years on average to find the proper key from a scrambled message.) However, since both parties in this type of cryptographic system need to have the secret key, the problem with this key system is with the secure transferring of the secret key.

Public key systems (asymmetric cryptographic systems) represent a new approach. Developed in the 1970s, this system generates two keys at the same time. One of the keys is known as the public key, which is then related to the secret key. It is practically impossible to decode the secret key by using the public key; therefore, each user can publish a public key, while keeping their private key secret. In short, this system works by allowing information encrypted with the private key to only be decrypted with the public key and vice versa. The most popular and formerly one of the strongest public

³⁴ Yaman Akdeniz et al., "Cryptography and Liberty: Can the Trusted Third Parties be Trusted? A Critique of the Recent UK Proposals" (1997) *Journal of Information, Law and Technology*, online: JILT <http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz/> (last modified: 27 June 1997).

key cryptography systems uses the RSA algorithm, which was developed in 1978. As RSA Data Security Inc. describes:

...an RSA key pair is created by multiplying two randomly chosen and very large prime numbers to arrive at their product (a modulus). The two prime numbers are used with the modulus to create the private and public keys.³⁵

Public key cryptography systems rely on the inability to factor large prime numbers rapidly and on the continuing inability of mathematicians to solve the long-standing problem of calculating discrete logarithms.

In general, the strength of encryption is related to the difficulty of discovering the key, which in turn depends on both the cipher used and the length of the key. A block cipher is a type of symmetric-key encryption algorithm that transforms a fixed-length block of plaintext (unencrypted text) data into a block of ciphertext (encrypted text) data of the same length. Encryption strength is often described in terms of the size of the keys used to perform the encryption. In general, longer keys provide stronger encryption. For example, 128-bit keys for use with the RC4 symmetric-key cipher³⁶ provide significantly better cryptographic protection than 40-bit keys for use with the same cipher. Roughly speaking, 128-bit RC4 encryption is 3×10^{26} times stronger than 40-bit RC4 encryption.

These technological advancements provide confidence, authentication, and integrity to documents and transactions that occur on-line. As a result, cryptography has created a more convenient way to transact. The growth of electronic commerce in

³⁵ *Ibid.*

³⁶ RC4 is a cipher invented by Ron Rivest, co-inventor of the RSA cipher, and is claimed as a proprietary system by RSADSI. It is proprietary in that RC4 is considered to be a trade secret of RSADSI. It is used in a number of commercial systems like Lotus Notes and secure Netscape.

Cyberspace and on closed networks (e.g.: debit card systems) is now measured in the trillions of dollars. Worldwide financial transfers through the Society for Worldwide Interbank Financial Telecommunications (SWIFT) network alone accounts for transactions currently estimated at approximately 30 billion dollars U.S. per year. While the estimates vary widely, with the skyrocketing growth of the Internet, and the subsequent number of users on-line, electronic revenues are projected to be about 440 billion dollars U.S. per year by 2002.³⁷

3.2 The Emergence of a Key Recovery System

Strong encryption (e.g.: a block cipher of 128-bits or better) is virtually unbreakable. It was estimated by James Bamford in *The Puzzle Palace: A Report on America's Most Secret Agency* that the cost of solving each solution (e.g.: finding the correct key of a single encrypted message) would cost \$200 septillion.³⁸ Consequently, although strong encryption can provide unparalleled informational security, if it is abused or misused the consequences can be equally as profound. As Dorothy Denning suggests:

It [encryption] has no safeguards to protect users and their organizations from accidents and abuse. It is like an automobile with no brakes, no seat belts, no pollution controls, no licence plate, and no way of getting in after you've locked your keys in the car.³⁹

In short, once this technology is deployed it is very hard to decode the information if you do not have the key. The Electronic Frontier Foundation (EFF) holds the world record in

³⁷ Task Force on Electronic Commerce, Industry Canada, *The Canadian Electronic Commerce Strategy* (1998), online: Industry Canada <<http://www.e-com.ic.gc.ca/english/60.html>> (last accessed: 11 March 2000).

³⁸ See generally James Bamford, *The Puzzle Palace: A Report on America's Most Secret Agency* (Boston: Mifflin, 1982).

³⁹ Dorothy E. Denning "The Future of Cryptography" in Brian D. Loader ed., *The Governance of Cyberspace* (London: Routledge, 1997) at 178.

breaking 56-bit encryption keys. Building a super computer, which utilized only available technology, worth \$150,000, the EFF was able to break the code after 22 hours and 15 minutes.⁴⁰ Currently, no one has yet reported to have decoded a 128-bit encryption (strong encryption) algorithm.

The development of strong encryption raises a perplexing tension between 'crypto anarchy' (e.g.: the idea that information can be sent via the Internet with no way for law enforcement to "control" illegal behavior) and state monitoring (e.g.: the government monitoring all private actions). Several alternatives may be used to balance interests. By the early 1990s key escrow encryption, also referred to as escrowed encryption, emerged and gained a great deal of attention. The idea is to combine strong encryption with an emergency decryption capability. This can be accomplished by linking encrypted data to a data recovery key that facilitates decryption. The actual key used for decryption in emergency cases would not necessarily be the actual decryption key; rather, it would act as some sort of 'master key'. This 'master key' is then held by a trusted fiduciary that could be a government agency, a court, or a trusted third party. Alternatively, keys may be split among several such agencies.

To safeguard users, key recovery systems may require that any investigative or intelligence agency make an application through appropriate procedures if it wanted access to communications or stored files. One such procedure includes obtaining a court order, which upon compliance would allow the investigative agency to receive the stored key. Moreover, these procedures could be done in such a way that the user would have no knowledge of the authorities' activities. This would be a critical part in the

⁴⁰ The EFF web page URL is: <<http://www.eff.com/>>.

investigative process, which facilitates the element of surprise, akin to a wiretap. In the end, escrow encryption systems would rely on access procedures, auditing and other safeguards in order to protect legitimate privacy interests.⁴¹

In 1993, the United States government realized that encryption technology was of paramount importance to the development of the Internet. The Clinton Administration announced several policy initiatives that would promote the use of encryption in a way that would balance the rights of citizens, the needs of businesses, and the ultimate requirements of law enforcement. In developing a policy that would meet these standards, the U.S. government also realized that it in no way wanted to prevent citizens from having access to encryption, or to stigmatize cryptography as something only criminals would use.⁴² As a result, the government developed an escrowed encryption system that was established under a single chip, the Clipper Chip.

The Clipper Chip was designed in such a way that each chip had its own unique key. The key, however, was split into two components, each of which would be held by two separate government agencies; namely, the National Institute of Standards and Technology and the Department of Treasury Automated System Division. As well, Clipper Chip's algorithm was the highly classified SKIPJACK, which had a key size of 80 bits, and was designed by the National Security Agency. In February 1994, the government adopted the Escrowed Encryption Standard, which is a voluntary government standard for telephone communications. Although the U.S. government was the first to act on this technology, it is not alone in the pursuit of key escrow technology.

⁴¹ *Supra* note 39 at 180.

⁴² *Ibid.* at 181.

Some type of key escrow is a feature or option of several commercial products that are produced by Nortel's Entrust, PC Security Stoplock KE, etc.⁴³

Several additional companies have proposed designs for commercial key escrow systems where the escrow agent is a trusted third party that would provide emergency decryption services. Although the requirements for private companies to act as trusted third parties have not been established nationally, or internationally, proposed conditions include licensing, or the ability of the organization to demonstrate its capability to administer key escrow encryption and safeguard keys.

Key escrow technology is often the center of debate when the use of encryption is employed. As Denning has commented, encryption (especially strong encryption) is virtually unbreakable⁴⁴, and as a result, when encryption is used, two primary concerns are raised. The first issue is with regards to law enforcement's needs to recover a key for criminal purposes. The second issue raised with the use of strong encryption is ensuring access by a company in the event that keys are lost or tampered with. These concerns are mitigated by the use of some form of emergency backup. Consequently, escrowing keys is arguably a vital component of the encryption process, especially if the minimum standard of encryption mandated is 128-bits or better. Ultimately, if it is virtually impossible to gain access to the encrypted message, the escrowing of keys will undoubtedly have to be addressed.

Escrowing keys could also – if legislated and/or implemented – have serious impacts on security, consumer protection, and in general, an impact on the acceptance of electronic commerce. In short, key escrowing raises questions such as; does storing keys

⁴³ *Ibid.* at 182.

compromise security? Is it in the best interest of consumers to use encryption if keys are escrowed? Will escrowing keys address the needs of on-line businesses? And, in general, will the adoption of key escrow technology help promote the intended electronic commerce infrastructure, both nationally and internationally?

The idea of escrowing keys from a security and business standpoint has been met with a great deal of debate. Aside from law enforcement and privacy issues, escrowing keys ensures that businesses have a backup key available for emergency situations. Furthermore, using escrowing agents can ensure the retrieval of information if the holder of the key dies or forgets the password. In this way the escrowing of keys provides a safety net for businesses and their consumers.

Although escrowing keys has its advantages, many have argued that storing keys would in itself compromise the security component that cryptography provides in the first place. It is argued that storing massive numbers of keys in the same place puts at risk all of the key holders. If the keys are exposed (e.g.: the escrow agent's files are hacked into), every key holder that escrowed their key would be at risk. Therefore, it is argued that in order to preserve the level of security that cryptography provides, each user should not share their key, even with an escrow agent. From a business standpoint, it is argued that companies have it in their own interest to store keys anyway. This partly stems from the fact that businesses themselves have a vested interest in backing up important keys in

⁴⁴ See generally *Ibid.*

order to safeguard their products and assets.⁴⁵ Hence, no government intervention is needed.

3.3 Assessment of Current Literature

Dorothy Denning (United States)

In addressing the encryption and key escrow debate in the United States, Denning has supported the idea of key escrow in order to avoid 'crypto anarchy'. Addressing this threat, it is maintained, requires an "international approach that provides for both secure international communications crossing national boundaries and electronic surveillance by governments of criminal terrorist activity taking place within their jurisdiction".⁴⁶ The adoption of an international approach, according to Denning, is of paramount importance. What's more, it is believed that key escrow has emerged as one approach that can meet the confidentiality and data recovery needs of organizations, while allowing law enforcement agencies to do their jobs. Also, escrowed encryption technology is able to facilitate the promulgation of standards and products that support the information security requirements of the global information infrastructure. In short, Denning argues that our information superhighways require responsible conduct.

While much of the opposition to escrowed technology comes from the belief that the government has an insatiable and unsavory desire to gather information about its law-abiding citizens, Denning responds by saying that this type of activity is unlikely.

While abuse of the Clipper system cannot be ruled out, it is unlikely. Neither the public nor Congress has tolerated such activity in the past, and federal wiretap laws, government

⁴⁵ This situation would occur if large businesses like banks operated on a 'closed' business certification authority model, for example. This would allow them to escrow the keys of their clients.

⁴⁶ *Supra* note 39. p. 189.

regulations and procedures, and congressional committees have been established to protect against their occurrence in the future. Wiretaps are conducted under tight controls and subject to considerable oversight. Clipper includes an additional layer of protection since anyone wishing to conduct a wiretap must also acquire a special decrypt processor and keys from the escrow agents.⁴⁷

Another critique of escrowed encryption that Denning addresses is the possibility that criminals will simply not use any type of escrow encryption, and thus avoid detection anyway. In response, she suggests that although criminals may in fact not use escrowed encryption, it is conceivable that over time, market forces could favor escrowed encryption such as the Clipper Chip. Organizations might require key escrow for their own protection, and vendors could favor it for its export advantage. As already mentioned, the government is utilizing key escrow products, and this could result in a demand for interoperability, which could lead to its proliferation. Consequently, criminals would have to choose key escrow because it would be more readily available to communicate with the rest of the world, and to facilitate their own emergency access.

Although Denning strongly suggests the use of escrowed encryption, she recognizes that key escrow is highly controversial and vehemently opposed by some proponents of encryption. Thus, its widespread adoption is by no means assured. Nevertheless, it is warned that if this technology were not adopted, the implications for the criminal justice system would be profound. Ultimately, she argues that the

⁴⁷ Dorothy Denning, "Resolving the Encryption Dilemma: The Case for Clipper" (July 1995), online: The Cryptography Project <<http://www.techreview.com/articles/july95/Denning.html>> (last accessed: 11 March 2000).

information society and the notion of a global electronic commerce market would be lost, and Cyberspace would become a safe haven for criminals.

From a security standpoint, Denning suggests that cryptography and escrowing keys will develop as a result of government use. Essentially, this argument assumes that government use of strong encryption and escrowing keys will promote this type of technology and that eventually, private firms and international firms will adopt this practice. She suggests that with clear government initiatives, consumers and businesses will accept key escrowing technology. As well, Denning does not seem to be worried about security being compromised as a result of key escrowing. In fact, she seems to be advocating the backing up of keys in the hands of the government as the most appropriate measure.

In fact, Denning suggests that several factors will facilitate the adoption of key escrow. First, it has been submitted that because key escrow products are exportable, under appropriate conditions, vendors will have a strong incentive to adopt key escrow systems. This incentive partly stems from the fact that it will allow for a single product line for both domestic and international sales. Moreover, Denning has implied that because the United States government has committed to escrow encryption, this will essentially ensure a large market for escrow products. Therefore, in order for businesses and consumers to keep up with the latest developments, the market will force more and more users to use escrowed encryption products.

Escrowing keys, however, under one agency, especially a government appointed agency, may have a far more profound impact than Denning suggests. To some measure, security will be compromised if all keys are held under one, or even several, agencies.

Keys are not only at risk from virtual 'hackers', but there is also some risk involved in having all keys stored in one physical location (e.g.: its location in the real world could also present security risks). As well, the potential for human error leaves at risk a large number of keys if they are all stored in one location. As a result, key escrowing security should also be evaluated from the perspective of physical security.⁴⁸

In the end, it is unlikely that consumers will adopt key escrow products simply because the government endorsed, or is using, this type of technology. Escrowing keys has been vehemently opposed partly because it is a clear invasion of privacy. It is quite possible that mandating escrow products will have a negative impact on electronic commerce in the sense that, not many consumers will be willing to compromise their informational privacy for law enforcement and/or national security needs. While consumers will welcome transactional security and consumer protection, it should not come at the cost of having to disclose the private key and leave a government agency or trusted third party with the ability to have access to all communications. Consequently, it is highly unlikely that key escrowing can be justified in the sense that, most people should not be coerced into using a government regime that retracts to a large extent several hard fought civil liberties (e.g.: freedom of association and freedom of expression).

Michael Froomkin (United States)

Implementing any kind of key recovery system would require the government to test the constitutional issues that such a system would raise. For example, a Canadian

⁴⁸ See generally Hal Abelson et al., "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption" (1998), online: CDT Encryption Issues Page <<http://www.cdt.org/crypto/risks98/>> (last modified: 30 July 1998).

government must take into account the *Charter of Rights and Freedoms* before instituting any mandatory system. In the American context, Froomkin has canvassed and surveyed the relevant parts of the U.S. Constitution. In doing so, he has specifically addressed the First, Fourth, and Fifth Amendments, as well as evolving conceptions of the constitutional right to privacy.

Froomkin has suggested that mandatory key escrowing may reduce associational freedoms, chill speech, and may constitute an intrusive search. Any such mandatory law might require a form of self-incrimination and would infringe personal privacy rights. However, under existing doctrine, Froomkin says that the analysis of the constitutionality of mandatory key escrow legislation would turn on the court's balancing of the potential costs to personal privacy against the perceived gains for law enforcement and national security.⁴⁹ On balance he claims that private, noncommercial users of encryption probably have a Fourth Amendment right to resist mandatory key escrow and might have a First Amendment claim as well.⁵⁰ It is less clear whether commercial users or corporations would have such rights under current doctrines.⁵¹

Froomkin also suggests that escrowing keys to trusted third parties right now (e.g.: in the absence of legislation) would be done at the risk of users and businesses. Without proper practices and/or legislation in place, trusted third parties are unreliable,

⁴⁹ Michael Froomkin, "The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution" (1995) 143 U. Penn. L. Rev. 709, online: Michael Froomkin's Homepage <<http://www.law.miami.edu/~froomkin/articles/clipper.htm>> (last accessed: 11 March 2000).

⁵⁰ See as well part of chapter 5 that deals with the constitutionality of export controls on encryption technology in the U.S. decision *Bernstein v. United States Department of State*.

⁵¹ *Supra* note 49.

and as a result, will affect the level of security provided or available. Therefore, Froomkin appears to be signifying that although the constitutionality of mandatory key escrowing will be for the courts to decide, without proper legislation and business practices, escrowing keys would in fact compromise security.

From the perspective of consumer protection, Froomkin's reliance on legislation for this type of technology may have some validity, in the sense that consumers would be protected to a large extent by the legal process. Nevertheless, the idea that business will provide emergency back-up decryption services (because they have a vested interest in doing so) may in fact be significant for this type of technology. As privacy concerns are often raised with the idea of escrowing keys, this is one area in which consumers and businesses have to take a leading role. To a large extent, if government takes on a leading role, consumers may be un-attracted to the benefits of doing business on-line (for fears of big brother). Conceivably, as well, mandating key recovery systems will stunt growth, partly because these types of systems will have to reflect the technology available in order to become effective. To this regard, consumer protection under a legislated regime will not necessarily be as efficient because of the inability of the law to keep up with advancements.

Legislating key escrow technology may also be unconstitutional within Canada. The *Canadian Charter of Rights and Freedoms* clearly outlines such freedoms as the right to reasonable search and seizure, the right to freedom of association, and freedom of expression. Although very little has been produced on this subject, and it is outside the scope of this work to accurately identify whether a Charter challenge will play a

significant role in the implementation of key escrow, these challenges should be seriously considered.

Yaman Akdeniz et al. (United Kingdom)

Most of the debate surrounding the use of cryptography has been whether or not individual users should protect their own key, or should each user have to provide some agent with a backup – e.g.: escrow the key to the government. Naturally, in the latter case individuals would be subject to some form of state monitoring. Despite these well-canvassed ideas, some have suggested alternatives, or what might be perceived as a modified version of escrow encryption. Akdeniz et al., for example, have proposed a key archiving alternative arguing that key escrow represents an unprecedented intrusion on individual privacy, which may hold back the development of digital communications and commerce, and which would not achieve the government's stated goals of helping to prevent crime.⁵² To more appropriately balance the outcome of encryption, Akdeniz et al. have suggested a system that they call 'key archiving'.

The key archiving system would work in the following manner. A request for an archival copy of a private key could be made by the citizen who has lost his or her key, by law enforcement after the arrest of a citizen for criminal activity, or by a family representative after a grant of probate if the citizen is dead. The trusted third party, on receipt of the request, publishes an electronic update invalidating the public key associated with the private key from all further use. A 'notice of revocation' is generated by the electronic updating system confirming that the public key has been invalidated. This notice becomes a key to unlock the registered trusted third party's key archive for

⁵² *Supra* note 34.

the recovery of the associated private key. Finally, the registered trusted third party recovers the private key from its archive using the 'notice of revocation'.⁵³

Hence, the use of a key archiving system enables the users and their correspondents to always know when a key has been revealed to the authorities. This they argue will help to prevent abuse of the system by persons inside or outside government agencies who lack proper authority to demand keys. Furthermore, the added protection of key invalidation once the key has been obtained, maintains, to some measure, personal privacy, autonomy, and security. They suggest that this system provides a sensible balance between the need for privacy and security in commercial affairs, and the genuine requirement of law enforcement (as well as the genuine requirement of businesses to safeguard themselves) to be able to prosecute wrongdoing.

In further supporting their idea of key archiving, and in rejecting traditional key escrow technology, Akdeniz et al. imply that ultimately we cannot have complete confidence in the trusted third parties or the law enforcement agencies that hold the copies of the encryption keys. In essence, this seems to be suggesting that the unparalleled level of security cryptography provides will be lost if traditional key escrowing is used. Although the key archiving system mainly deals with individual privacy rights concerning key escrowing, from a security standpoint, it does little in dealing with the issue of the protection of keys. For example, this alternative does not seem to be concerned with the escrow agent's vulnerability to hackers, or physical security risks. Notwithstanding this realization, key archiving does seem to provide added security to key escrowing by at least notifying individual users when their private

⁵³ *Ibid.*

key has been released. To some measure, this information will help protect users and businesses.

Nevertheless, key archiving does little to improve consumer protection for electronic transactions, and little to help promote electronic commerce in general. Key archiving is essentially a modified version of key escrowing and in the end does not deal effectively with privacy concerns, as well as security concerns. Consumers still have their privacy rights swaying in the balance, and security concerns of the agent who will hold the keys are still undetermined. Further, it is still unclear as to whether consumers will find this type of technology attractive – especially when businesses can, to some degree, provide more effective and faster solutions to transactional problems. Consequently, the key archiving system is probably a more complex system (at least technologically) that does little to improve security and consumer protection.

Hal Abelson et al.

Since 1996 Abelson et al. have reported on the issues of encryption, key escrowing, and trusted third parties. Their report entitled, *The Risks of "Key Recovery", "Key Escrow", and "Trusted Third Party" Encryption*⁵⁴, written by a team of computer scientists and engineers, has maintained that its finding (that key escrow poses a security risk) have yet to be substantively challenged. In their 1998 report they have continued to suggest that any form of key escrowing or key recovery is expensive, and ultimately undesirable. In coming to this conclusion, they have commented on the technical risks, costs, and implications of deploying a system that provides government access to encryption keys.

⁵⁴ *Supra* note 48.

They maintain that escrowing encryption keys will result in substantial sacrifices in security and increase costs to the end-users.

They suggest that sacrifices in security come from the fact that keys will be stored, and thus are vulnerable to theft. Increasing the number of people with authorized access to the critical infrastructure and to business data will increase the likelihood of attack, whether through technical means, by the exploitation of mistakes, or through corruption. Moreover, they also advise that key recovery requirements, to the extent that they make encryption cumbersome and expensive, can have the effect of discouraging or delaying the deployment of cryptography in increasingly vulnerable computing and communication networks. In essence, key recovery will slow down the process of secure data flow – e.g.: electronic commerce.

Additionally, they suggest that building a key recovery system with adequate technological underpinnings demanded by the key recovery system is complex and far beyond the experience and current competency of the field. Although it may be possible to make key recovery reasonably transparent to the end users of encryption, a fully functional key recovery infrastructure is an extraordinarily complex system, with numerous new entities, keys, operational requirements, and interactions. In the end, the key recovery aspects of such a system are far more complex and difficult to implement than the basic encryption functions themselves.

As well, even if such infrastructures could be built, the risks and costs of such an operating environment may ultimately prove unacceptable, in that, it would generally require extraordinary levels of human trustworthiness. Consequently, Abelson et al. suggest that the onus is on those who advocate key recovery to make the case that the

benefits outweigh these substantial risks and costs. Further, they have maintained that industry will not need key recovery because they will protect themselves – e.g.: they will back up encrypted data themselves.

It is clear, at least at the present time, that advocates of key recovery have not made a sound case for the implementation of this technology, especially if this type of system will require extraordinary technical knowledge and structure. To this end, mandating key escrow is unfeasible for the simple reason that it is not technically possible to build such a system – at least for now. As well, it is clear that such a system would not only require a great deal of technical knowledge, but it will more than likely increase the costs to end users. As a result, if government policy mandated such a system, it would be extremely difficult for private industry to build the system and it would also increase costs to end users, which will not help in the promotion of electronic commerce. In short, this particular analysis of key escrowing suggests rightfully so, that privacy, and perchance security issues, may not be the primary problem with key escrow technology; technological issues are.

Mandating the use of key escrow technology, while promoted by Denning and to a lesser degree by Akdeniz et al., is unlikely for several reasons. First, key escrow systems are at the present time undesirable because they represent an intrusion on personal privacy. Second, key escrow systems are at present time technologically complex and will substantially raise costs to end-users. As well, there has yet to be a convincing argument that illustrates that the benefits of such a system out-weight the costs end-users will endure. For now, these circumstances will not help promote

electronic commerce, and as a result should discourage government from mandating key escrowing systems.

3.4 Canada's Cryptography Policy

Canada's cryptography policy prior to October 1998 did not restrict or control the import, production or use of any strength of cryptographic products within Canada. However, Canada was, and still is, a member of the 33 nation Wassenaar Arrangement⁵⁵ under which it is obliged to control the export of hardware and some software cryptography products, as well as products that use cryptography. Although there have been no restrictions on the use of cryptography within Canada, the various restrictions on the export of cryptography have had a major impact on this influential industry that is emerging within Canadian borders.

In essence, the regulations that were put in place under the Wassenaar Arrangement were to help prevent the movement of certain goods that may not be in the strategic interest of Canada or its allies. Nevertheless, Canada has recognized that certain cryptographic goods are legitimate, and as such, has suggested that its cryptography policy needs to represent the needs of distributing these goods outside of Canada in order to make Canada a world leader in this technology. In particular, Canada has acknowledged the need for the widespread distribution of digital signature technology in order to properly facilitate and promote electronic commerce.⁵⁶ As a result, Canada has articulated that these products be available for export with little or no restrictions.⁵⁷

⁵⁵ The details of this arrangement will be fully explored in chapter 5.

⁵⁶ See generally *Supra* note 37.

⁵⁷ This statement was given in the Honorable John Manley's (Minister of Industry) speech on October 1, 1998, online: Task Force on Electronic Commerce <<http://e-com.ic.gc.ca/english/speeches/42d3.htm>> (last accessed: 11 March 2000).

In developing its latest cryptography policy, the Canadian government adopted a thorough consultation process with the goals of identifying a solution to these very complex issues. The consultation process confirmed that the issues and concerns already raised by various groups needed to be addressed. Businesses wanted the cryptography policy to help protect their network transactions. They also raised issues such as the need to protect intellectual property, and corporate databases. Finally, they suggested that they wanted to fund and develop their own security initiatives, rather than have government dictate the course of action.

Consumers wanted the cryptography policy to allow for affordable software. As well, consumers wanted to be able to decide what product they use. While civil liberty organizations and privacy advocates echoed these sentiments, they maintained that mandatory key recovery or key escrowed systems be discouraged. Conversely, law enforcement wanted some form of timely access to encrypted data. Further, in supporting this claim, law enforcement agencies submitted that they are not looking for increased investigative capabilities or new authorities, they merely want to restore and maintain what was available before.⁵⁸

After taking all of the interests into consideration, the Canadian government decided to deliver a six-point cryptography policy.⁵⁹ First, it affirmed the right of Canadian citizens to develop, import and use whatever cryptography technology they wished. In doing so, the Canadian government felt that Canadians should have access to whatever type of cryptography they feel is necessary, up to and including the use of strong encrypted products. Second, the government decided that it would not implement

⁵⁸ *Ibid.*

or legislate any form of mandatory key recovery system. Likewise, it decided that any form of licensing requirements for certification authorities or trusted third parties was not necessary.

As a result, the government decided that it would let private industry establish responsible practices in these areas. They asserted that this will build consumer and business confidence in these products and services, and will assure business continuities in cases of lost or corrupted keys. In the end, the government suggested that it would use government procurement to encourage commercial key back up. At the same time, however, the government prolonged its commitment to the Wassenaar Arrangement, but assured that it would be done in such a way that Canadian cryptography manufacturers would face a level playing field. Fifth, the government proposed to streamline the export permit process to make it more transparent. Its intention in doing so was to simplify and speed up decision-making, and to significantly reduce the 'regulatory drag' on exporters.

In its sixth point on cryptography technology the government proposed a substantive change to the *Criminal Code of Canada*. This included making it an offence to wrongfully disclose private encryption key information, and making it an offence to use cryptography to commit or hide evidence of a crime. The main policy consideration behind this proposed change was that this will protect consumers' privacy and will also give law enforcement agencies and national security agencies the legal framework they need to ensure public safety. In the end, the government maintained that this policy supports electronic commerce in Canada because it provides tools for privacy protection that will help implement forthcoming legislation.

⁵⁹ *Ibid.*

As well, the government articulated that this policy encourages the use of information technologies to protect business transactions, critical infrastructures, and ultimately in preventing economic espionage. Hence, the government implied that this policy underscores that Canada is “open for electronic business”. Furthermore, the current policy encourages the widespread use of strong encryption, and consequently, the growth of export markets for Canadian technologies.

3.5 Assessment of Canada’s Cryptography Policy

The latest cryptography policy initiatives presented by the Canadian government reflect, to a large extent, some of the major concerns and issues raised in the academic literature. What is more, the latest policy illustrates that the Canadian government will allow consumers and businesses to decide what type of product they wish to use. As a result, the policies delivered in October of 1998 contained little substantive content. It is quite apparent that the Canadian government for now will allow market forces to dictate the course of action.

Whether this is an advantageous course of action has yet to be determined. Certainly academics like Denning and Akdeniz would suggest that the failure to mandate key recovery might have profound effects on the Canadian criminal justice system. Nevertheless, the Canadian government has deemed that the best course of action is to allow consumers and businesses to determine what is best for the growth and development of electronic commerce.

Mandating key escrow technology, at least at the present time, undermines civil liberties and has therefore been vehemently opposed. To require that private citizens who use encryption software leave a ‘master key’ in the hands of a government agency or

private third party, strikes fear that the right to privacy will be compromised. Leaving this issue aside, legislating the use of this technology is unnecessary to encourage electronic commerce.

From a business and security perspective, some use of key escrowing is a good business practice. Good business standards dictate that a firm protects itself by archiving transactional information. For example, businesses would archive their own keys and would take steps to obtain the private key of their customers (which they would easily have access to under a 'closed' certification authority business model). Even in the paper world this practice has been implemented for many years now. Consequently, Canada's cryptography policy that mandatory key escrow technology is unnecessary is correct, partly because in the long run businesses will in fact mandate for themselves policies and strategies that are far more advanced than those that could reasonably be mandated by government.

What is more, key escrow legislation would not promote an electronic commerce infrastructure. Such an infrastructure would in essence ask citizens to give up a certain amount of informational privacy by allowing government to monitor all transactions – or to at least give governments the capability of doing so. While the majority could conceivably oppose this, in the end key escrow does little to help create certainty in transactions, which is of great importance in facilitating a strong on-line security standard. Thus, it is clear that key escrow technology is not a standard that government should implement because it will not facilitate or support the appropriate infrastructure electronic commerce needs.

More important is the encryption level (e.g.: key length) at which consumers and businesses operate on-line. As 56-bit encryption keys are now breakable, consumers are increasingly vulnerable to hackers. In the near future, 56-bit encryption keys will only become easier to decode by hackers as technology advances, and this will inevitably lead to an increasingly insecure electronic infrastructure. To some measure, in order to facilitate a secure infrastructure, government should be mandating minimum length encryption in order to ensure the safety of data in all transactions.

This is the less controversial aspect of data security, but it is essential to ensuring transactional security. Moreover, this is an important question that the Canadian government did not address in its speech in October of 1998 on cryptography technology. It is important that a minimum level of security be met in order to promote electronic commerce. Moreover, this minimum level or standard is in the interest of everyone involved, yet, at the same time has avoided specific consideration from both academics and government.

More to the point, citizens and businesses must have, from a business standpoint, a basic security level by which to operate on-line. Regardless of the danger to privacy from key escrowing, strong legislated Canadian encryption standards will provide a degree of certainty for all consumers and businesses within Canada. Moreover, a minimum encryption level can help promote open and fair competition. This in turn will promote data sharing and on-line transactions, and it will also suggest that 'Canada is open for business'. It will demonstrate Canada's willingness to integrate its economy into the global economy, while at the same time maintaining sovereign control over the direction of its economy. Accordingly, the Canadian government in its consultations on

cryptography should have asked a more specific question; namely, should key length be mandated? To a large extent domestic key lengths will have to match international requirements, nevertheless, establishing a minimum key size in Canada in accordance with minimum key sizes internationally will foster democratic and sovereign principles, and ultimately establish certainty in transactions domestically.

4. SECURITY IN TRANSACTIONS: LEGISLATED STANDARDS VS. INDUSTRY DEVELOPED STANDARDS

This chapter discusses the use of digital signatures, certification authorities, and public key infrastructures. Each technology is described, followed by an analysis of the perils and potential in implementing these technologies in private and public systems domestically and internationally. Within each section, two viewpoints will be canvassed in order to make an assessment as to the role of government in establishing security standards within each of the technologies.

Some commentators argue for government legislated minimum standards for security. They argue that this will help protect consumers' interests, and create the needed international interoperability. Other commentators argue that legislative intervention will distort innovation. They also argue that legislative regulation will deter interoperability. The detailed analysis of these perspectives leads to the conclusion in this chapter that government intervention through legislation may only be necessary with regard to key length, and to some extent procedural requirements for CAs, in order to develop and implement these vital technologies into a secure electronic commerce infrastructure.

4.1 Digital Signatures

In most countries paper-based documents are usually required by law to satisfy a number of transactions. For example, there are requirements in legislation that stipulate certain documents be 'notarized' or 'signed'. These kinds of provisions presuppose the existence of paper documents that in the world of Cyberspace do not generally exist. Since the advent of new electronic media and the Internet, businesses have attempted to minimize the effects of legislation biased towards paper-based transactions. In effect,

businesses entered into contracts with their trading partners in which they established how business would be transacted via electronic technology. Understandably there are limitations to these arrangements – such as the best evidence rule that is in force in many common law jurisdictions – which takes into account the presentation of an original copy. In essence, these arrangements are utilized to fulfill a perceived or real gap in the law.

The development of public key cryptography allows participants to determine with certainty who each of the other participants are, and to establish that an identifiable sender sent certain documents transmitted electronically. Participants can also use public key cryptography to assure themselves that the contents of the electronic document remain confidential. In addition to the authentication and non-repudiation functions, public key cryptography provides users with some form of integrity in the form of digital signatures.

From a technical perspective, digital signatures function by having the sender create a hash algorithm. For example, if person A wants to send a message to person B and have their digital signature attached they would begin by sending the message through a mathematical function known as a hash function. This hash function provides a summary (hash code) of the message person A is sending. This summary hash code is unique to each message, and person A would then encrypt the hash code using his/her own private key and attach the hash code, or digital signature, to the end of the message. When person B received the message they could de-crypt the message using their own private key. Then they would de-crypt the digital signature using the public key of person A in order to get the hash code. Person B would then pass the message through

the same hash code, and if the two hash codes were the same, then person B could be certain that the message that was sent, had not been altered.⁶⁰

The unparalleled level of integrity that digital signatures provide in electronic commerce means that various forms of 'spoofing'⁶¹ and 'hacking' can be restricted. Digital signatures provide a means whereby consumers, businesses, and even governments can verify whether or not a message has been manipulated. This is an integral component for the growth of electronic commerce, and although many governments have taken initial steps to adjust their respective legal frameworks to recognize the use of electronic documents, there remain a number of legal and policy issues un-addressed with regard to this technology.

The United Nations Commission on International Trade Law (UNCITRAL) undertook the study of digital signatures in part to help promote harmonized statutory reform. Although a number of other organizations have also undertaken such steps, UNCITRAL is recognized as one of the most important international forums for discussions of electronic commerce issues.⁶² UNCITRAL was thrust to the forefront of electronic commerce policy making in large part due to its mandate to prepare legal texts for the purposes of harmonization.

⁶⁰ E. Michael Power, "Digital Signatures and Public Key Encryption Presentation" (1998), online: Treasury Board of Canada Secretariat Chief Information Officer <http://www.cio-dpi.gc.ca/pki/Downloads/Signatures/signatures_e.rtf> (last accessed: 11 March 2000).

⁶¹ This generally refers to the interception, alteration, and retransmission of a cipher signal or data that misleads the recipient of an encrypted message.

⁶² Canada, "Report of Canadian Delegation on the Thirty-fourth Session of the UNCITRAL Working Group on Electronic Commerce" (1999), online: Department of Justice Canada <<http://canada.justice.gc.ca/en/ps/ec/un99gau.html>> (last accessed: 11 March 2000).

This powerful mandate of UNCITRAL resulted in the approval of a Model Law in 1996. The Model Law's purpose was to make legal systems media and technology friendly. More to the point, its task was to provide a framework of default rules that address the validation and recognition of contracts on-line. This Model Law approved by UNCITRAL in 1996 has been widely accepted by many countries, including several states in the United States and in Canada. In fact, the Model Law in part inspired the federal government's Bill C-54 "The Personal Information and Electronic Documents Act".⁶³

The Model Law did not specifically address the issue of digital signature requirements; consequently, UNCITRAL developed a "DRAFT Uniform Rules on Electronic Signatures" in 1998. The working group set up to study digital signature issues began work in February of 1997, and by February of 1999 had convened for its fourth time. This add-on to the Model Law adopted a 'functional equivalence' approach. This meant that the law proposed by UNCITRAL would recognize with the same legal effect electronic documents, as it would paper-based documents.⁶⁴

The project had, and continues to have, three principal areas of research. First, the working group aims to prescribe a class of signing methods that could be deemed, or presumed to be, "appropriately reliable" for a broad range of signature requirements. Second, the working group intended to set out the obligations in relation to the determination of the identity of the signatory of a digitally signed message, the recipient

⁶³ *Ibid.*

⁶⁴ *Ibid.*

of the message, and the certification authority. Finally, the group is considering how to facilitate recognition of a digital signature made by a foreign signatory.⁶⁵

When the group first met it thought that the best legal framework for digital signatures would resemble the Utah Digital Signature Act.⁶⁶ This Act quite simply outlined the responsibilities of the signer, the relying party, and a trusted third party. In short, it was assumed at this point that a trusted third party was necessary for this type of technology to operate legally, or even technically. Although this tripartite structure for digital signature technology was recognized widely even in academic literature at the time, it was soon accepted that not all countries would adopt a three party model. Moreover, the group wanted the Model Law to be technologically neutral so as not to stunt innovation.

UNCITRAL abandoned the term digital signature because it presupposed a three party system. Alternatively, the UNCITRAL adopted the term 'enhanced electronic signature'. By 1998, however, innovation started to hamper even this perceived technologically neutral term. Alternatives to the technology became available, which in short, began once again to question the UNCITRAL terminology. (For example, digital signature technology became available that essentially did not require a trusted third party⁶⁷)

The meeting in February of 1999 ended with an agreement between the Commission and the delegates that their work on the development of legal rules concerning digital signatures is of great importance. It was agreed that any impediments

⁶⁵ *Ibid.*

⁶⁶ Utah Code Ann. 5 46-3-201 (1996).

⁶⁷ *Supra* note 62.

to international electronic commerce need to be avoided as soon as possible in order to ensure the growth of the industry. The work of UNCITRAL is recognized as a work in progress. As such, the draft on digital signature rules may eventually provide effective guidance in promoting standards for electronic commerce.

The use of digital signature technology in Cyberspace is important because digital signatures will provide a replacement for the traditional legal functions of paper and ink in the real world. This technology is therefore vitally important to electronic commerce and will understandably play a large role in establishing contractual relationships on-line. Notwithstanding the Canadian government's role in the UNCITRAL proceedings, and its consultation papers on digital signatures, Canadian citizens have yet to have a clear opportunity to address and articulate their views as to the development of this technology. This is partly because most people within Canada regard this technology to be in its infancy, and because not many people fully understand the technology or its possible impacts.

UNCITRAL's working group is focused on preparing legislation related to the procedural requirements for digital signatures. Although these requirements constitute an essential part of promoting electronic commerce, both domestically and internationally, the technical aspects of security regarding digital signatures have been overlooked. As well, UNCITRAL has over-looked the possible distinction between different levels of security policies for digital signatures. The level of encryption security also needs to be addressed to ensure effective use of the technology.

Addressing key length does not compromise UNCITRAL's goal of technological neutrality. Rather than promoting a particular technology, it promotes a minimum level

of security. Digital signatures are of paramount importance for electronic commerce because they provide integrity with regard to electronic documents. In assuring that this integrity is achieved, addressing the encryption level used for digital signature technology is important.

Failure to have sound technological underpinnings for digital signature technology may be dangerous. Failure to use digital signatures with strong encryption algorithms allows hackers the opportunity to manipulate sensitive data. In essence this compromises the integrity that digital signatures are being used for in the first place. Consequently, if digital signatures can be altered and/or copied by intervening third parties, they will not be able to carry out the legal functions that they are supposed to provide in Cyberspace. In the end, contractual relationship between any two parties on-line will be unlikely.

Enacting legislation that stipulates a minimum key length for digital signature technology will understandably raise a variety of concerns, particularly because of industry's interest in leading the way technologically. Clearly, industry led standards regarding security fosters innovation. To this end, government intervention would clearly stymie improvement in technology at a time when Cyberspace technology development is at a peak. As well, government may be unable to keep up with such a fast moving industry and as a result any government regulation would only hamper modernization. At the same time private firms developing the technology would have to slow down their production and innovation lines in order for government to respond to both the legal and policy aspects of the technology they are developing. By allowing consumers to choose, however, innovation would be sustained and it would also create a

more synergistic link between consumers and businesses. It is this link that may provide appropriate standards.

On the other hand there are concerns with regard to the ability of private industry in providing consumers with the necessary protection that digital signatures require. In short, to what extent do businesses strive to protect consumers' interests? If, for example, a firm doing business on-line finds itself financially burdened, will consumer security be compromised? If it were, consumers would find their digital signatures are being manipulated. To this regard, hackers may be able to make on-line purchases without the consumer even being aware of any activity. If the digital signature were taken as legal authorization, the consumer would have no redress. Perhaps to some degree, firms themselves have a vested interest in protecting their own digital signature. Nevertheless, it is the consumer that remains the most vulnerable. The protection of one's own signature from intervening third parties on-line is a service that transcends private industries ability to deliver.

Digital signature legislation raises concerns nonetheless. Having to establish a secure and recent encryption infrastructure (or even any encryption infrastructure) for smaller on-line businesses could prove costly. In this sense, if a minimum standard of encryption were legislated it could have an impact on the nature of on-line businesses. Only larger and more powerful businesses may be able to afford to be on-line. Moreover, many digital signatures and transactions on-line may not need strong encryption levels. Consequently, it would seem unnecessary for a law to dictate that a certain level of encryption be used for routine transactions where little or no monetary funds are transferred.

Legislated standards, however, go beyond these concerns because they provide the necessary protection that digital signature technology needs. Legislation would in fact provide a basis for uniform rules, both domestically and internationally. The UNCITRAL Model Law shows that current legal frameworks should accommodate new technology and new ways of doing business. Governments, in a way that industry cannot match, can uniformly implement procedural, and more importantly, basic technical rules, that are so crucially necessary for digital signatures to hold the legal significance that paper and ink hold in the real world. As a result, UNCITRAL and other organizations (in particular domestic governments) should not over-look key length legislation to help establish this legal confidence.

As well as providing consumer protection, mandating longer key lengths for digital signatures will more than likely be attractive to end-users in the sense that most citizens, to the extent that they understand the consequences, would welcome the unparalleled level of transactional security and privacy. Furthermore, if longer keys were mandated, fears of doing business or engaging in contractual relationships on-line may be reduced. The Canadian government should have specifically addressed this issue in order to provide the certainty and integrity that digital signatures can offer. It must regulate both procedural requirements, and basic technical requirements to ensure transactional security.

A close look at Bill C-6, The Personal Information Protection and Electronic Documents Act⁶⁸ (introduced in the House of Commons on October 1, 1998 as Bill C-54)

⁶⁸ Bill C-6 *Information Protection and Electronic Documents Act*, 2nd Sess., 36th Parliament, Canada, 1999.

illustrates that the federal Government of Canada may soon regulate the technical requirements for digital signatures. In Bill C-6 the government has recognized the need for secure electronic signatures, and has defined this to mean an electronic signature that results from the application of a technology or process regulated by the Governor in Council. Section 48 gives the Governor in Council the power to prescribe a technology or process for the purpose of ensuring that electronic signatures are secure.

In short, Bill C-6 now gives the federal government the power it needs to regulate not only procedural but also technical aspects of digital signatures. Since this is the case, one aspect of digital signature technology that the government should address is key length. Ensuring the safety of on-line consumers will begin with the recognition of safe minimum technological standards.

4.2 Certification Authorities

The use of public key cryptography, and its more specific application of digital authentication, undoubtedly allows electronic commerce transactions to operate under secure protocols. Another key component in providing a secure infrastructure however is that of a certification authority (CA). The role of the certification authority is to provide certainty to the identity of the person who owns a public key. In short, it is the certification authority that will not only distribute the public keys for users, but each CA will be able to indicate to whom the public key really belongs. From a technical perspective, the certification authority becomes engaged in the process by issuing a certificate. It is on this certificate (which is encrypted) that the public and private keys of a particular person are located. Prior to issuance, however, the CA would verify the person's identity, and then issue a certificate in that person's name.

In short, the CA's responsibility is to establish the true identity of the person using the encryption key. For example, without the use of CAs, person A could create his or her own random encryption key and then assume a false identity. Person A could then make transactions on-line using the stolen credit card number of person B, however, person C (the vender) would have no way of really knowing if the person they were transacting with was person B or not. As a result, in order to establish the connection between the sender of the encrypted message and the identity of the person who uses that particular key, a CA needs to be contacted to verify that person B is the only one who has access to that particular key.

There are a variety of complex legal and policy issues that surround the implementation of certification authorities – also known as trusted third parties. The root of this debate is whether or not to have a trusted third party (e.g.: closed community CA structures allow for parties to play several roles, meaning that a third party may not be required⁶⁹). As well, debates have surrounded the issue of who should act as the certification authority, a government agency or private organization? Of recent concern however, are issues over accreditation; namely, how should the accreditation of CAs operating in different business models be accomplished knowing that each certification authority environment is unique?⁷⁰

⁶⁹ *Supra* note 62.

⁷⁰ See generally Industry Canada, *Electronic Authentication Policy Workshop Working Paper* (Ottawa: November 22, 1999).

The two basic CA business models identified by Domus Software Limited and Industry Canada are open community CAs, and closed community CAs.⁷¹ Open community CAs can be classified as those CAs that operate with no contractual privity between the parties (the key holders) and the CA. Further, a CA under this business model is an independent legal entity with respect to its individual subscribers and relying parties. Consequently, the certificates issued by an open community CA are intended for use by other distinct legal entities. A specific example of this type of CA would be a commercial network service provider who issues certificates to people who have paid a subscription fee. In short, as subscribers sign transactions on-line, the relying party would verify with the open community CA that the subscribers are who they say they are – undoubtedly using a certain amount of trust in doing so.

Under a closed community CA business model there is contractual privity between the relying party and the CA. The closed CA business model assumes that the party who relies upon a given certificate is also responsible for the issuing of the certificate. More to the point, it is the CA who is also the relying party. As a result, the certification authority and the subscribers are all part of one legal entity. Further, under this model, the relying party (the CA) has control over the issuance of certificates, and also has control of the process whereby initial identification and registration is accomplished. Most often in the case of closed community CA models, the issuing of

⁷¹ Report to Industry Canada by Domus Software, “Certification and Accreditation for PKIs and Certification Authorities: Survey of Standards, Trends and Identification of Potential Models” (1998) Version 2.1, online: Domus Security <http://www.domus.com/onsecurity/industry_can.pdf> (last accessed: 11 March 2000) at 15.

certificates is for a purely technical purpose.⁷² That is, the certificate is usually to allow financial transactions with a single public key – such as would be the case with banks.

The Internet Engineering Task Force PKIX part 4 framework identifies a third possible business model for certification authorities.⁷³ This model stipulates that the CA would operate under an open but bounded structure. Unlike the closed system, multiple parties could rely upon a certificate under this model. Nevertheless, there would be limits placed upon the parties that could rely on the certificate – unlike the open model. Reliance is achieved under this type of model by the limits that are set and enforceable by bounding the possible parties and uses of certificates and technical processes.

The possible risks and liabilities (for both users and CAs) associated with an open community certification authority are much higher than that of a closed community CA. With the implementation of a closed community CA there is an opportunity for firms to reduce risk and liability by allowing other components of the business model to mitigate risk. One example of a mitigating factor could be the implementation of a fraud detection mechanism.⁷⁴ As such, perhaps the selection of accreditation schemes should take into account the full package of the business models in order to fully balance the requirements for accrediting a CA. As Domus and Industry Canada have concluded, if closed community models are adopted, government intervention should only occur if it can be clearly demonstrated that there is a failure in the marketplace (e.g.: conditions exist under

⁷² *Ibid.* at 16.

⁷³ Internet Engineering Task Force PKIX, *Certificate Policy and Certification Practice Framework Part 4*, online: IETF Homepage <<http://www.ietf.org>> (last access: 11 March 2000).

⁷⁴ For example, software that would automatically detect fraud or any other misconduct.

which digital signatures are deemed not secure enough for effective proof of identity or legal recognition).⁷⁵

At the same time, Domus and Industry Canada suggest that caution is warranted if governments decide to intervene into any type of model. They suggest that legal recognition of electronic authentication solutions should essentially support the maintenance of existing business models, and build upon those foundations. As a result, any government intervention should be based upon the recognition of and use of the existing business relationships, and not a redefinition of existing business models. They caution as well that government intervention should only occur if there is no contractual privity between relying parties and the firms (open CA structures); or the effective proof of identity is provided by a third party.⁷⁶

The alternative to either government intervention or industry developed accreditation schemes is to have a combination of both. This would involve the development of some form of minimum standard approach for CA practices, or the establishment of one or more accreditation method. A standards based approach has a number of viable functions. First, a standards based approach could help facilitate mutual recognition of electronic signatures generated by different policy and legal jurisdictions. As well, it could enable consumers to make meaningful comparisons and informed choices about whom they are doing business with. In the end, standards will result in the necessary commonality needed to accommodate the interoperability that

⁷⁵ *Supra* note 71 at 17.

⁷⁶ *Ibid.* at 18.

consumers expect.⁷⁷ Nevertheless, while standards help promote open and fair competition, there would also have to be recognition that innovation must not be distorted. Accordingly, it has been suggested that standards be led by the private sector to ensure relevance and effective consensual agreements among users.⁷⁸

Notwithstanding the benefits of a standards based approach to certification authorities, a high level of accreditation will be necessary to support consumer's interests. Developing any scheme for accreditation will understandably require the input of many interested parties, each having interest in, and helping to develop, a certain area of the model. Quite possibly, any accreditation scheme developed will be created by private industry, but manufactured in such a way as to meet a well-defined requirement. Whatever the approach, the model will need to be flexible enough so as to meet the satisfaction of many national and international business requirements, as the basic objective of accreditation will be to formalize trustworthiness of CAs across a variety of interested parties. More to the point, accreditation will validate contractual relationships between different closed community CAs.⁷⁹

Even a high level of accreditation leaves open the issue of liability that each CA can confront. Accordingly, the case for legislation regarding CAs could be re-affirmed partly because of the lack of clear rules regarding liability. Uncertainty with regard to these rules increases costs and discourages transactions that in the end threaten the production capacity of CAs for issuing certificates. As well, absent legislation for CAs

⁷⁷ M. Geist, "Approaches to Self-Regulatory Accreditation Schemes" (1999) Panel 2 in Industry Canada, *Electronic Authentication Policy Workshop Working Paper* (Ottawa: November 22, 1999) at 4.

⁷⁸ *Ibid.* at 4.

⁷⁹ *Ibid.* at 5.

and end users liability, the cost of insurance would be so enormous that it would in turn create disincentives for those wishing to do business on-line. Legislation, however, may help to protect consumers in that a statute can require a CA to carry insurance or reserves to meet any claims for their errors.⁸⁰

Further, legislation regarding liability may in the end help create the interoperability consumers are looking for. Although it is not unreasonable for users to grade certificates according to the liability regime that may apply to that certificate, it would be unreasonable to assume that consumers would take into account factors such as the effect of the geographical location of the CA and the trading parties on the choice of law. Users cannot be expected to keep abreast of changes in law in multiple jurisdictions, nor can they be expected to have such information accessible to them. As Michael Froomkin has suggested:

One can imagine the introduction of yet another intermediary that would perform this rating function, but requiring the introduction of a trusted fourth party to rate trusted third parties seems to be too much of a good thing. A uniform national or even international rule would be much easier to understand and to administer.⁸¹

The case against legislation regarding the liability of CAs addresses this concern by indicating that legislation would be to a large extent premature. Perhaps, as well, unfair, in the sense that commercial CAs are so new that the industry has barely had a chance to react. In essence, the market is at a stage where few CAs, clients, and certificates exist, and as a result, there is little basis to predict with sufficient precision as to what will happen with the technology, or the draft rules that do exist. Similarly, it

⁸⁰ Michael Froomkin, "The Essential Role of Trusted Third Parties in Electronic Commerce" (1996) 75 Oregon Law Review. 49 at 108.

could be argued that if standardized rules were implemented before the market for certificate policies has had a chance to reach equilibrium, the government would usurp fair rules created from competition between states and provinces, which in the end are better suited than any government standard.⁸²

The concern over government intervention regarding certification authorities, particularly surrounding the issues of accreditation and liability, will certainly have a profound impact upon the growth and acceptance of electronic commerce. Despite the infancy of the market vis-à-vis this technology, accreditation and liability standards are conceivably areas where the market will not live up to the appropriate and necessary principles consumers will expect. To this regard, certificates must reasonably engender reliance if public key cryptography is used in electronic commerce. If they do not, public key cryptography will not present the new global economy with a secure technological way of transacting. Although the market may be able to offer a technological infrastructure for the operation of CAs, it may not have the ability to provide and establish procedures that are in the best interest of consumers. This may become a reality partly because the market is driven by profit, and as a result, consumer protection may not necessarily be the primary motive in establishing CA standards – if standards were even deemed as being important by private firms. In short, certificates may resemble a component so vital to electronic commerce, that their procedural requirements (in the best interest of users) may need to be legislated. Consequently, government legislation outlining specific rules for accreditation and liability might be necessary in the near future in order to foster interest in electronic commerce.

⁸¹ *Ibid.* at 110.

Although businesses seem, at least for now, wary of legislation,⁸³ maybe in the long term firms will praise the implementation of government standards in this area. After all, if accreditation and liability schemes are implemented by private industry, consumers may in fact simply look to existing trusted bodies to provide them with the assurances they require in the on-line world. This would be done partly because consumers may prefer a great deal of transparency in the system they choose (e.g.: a system that would require no technical knowledge) for digital authentication. The question that remains is, is such an oligopolized system appropriate? Legislation in this area could in essence open the market, allowing a number of vendors to maximize their choice in the marketplace.⁸⁴

4.3 Public Key Infrastructures

It is too early to indicate the types of policies and practices that will be implemented or developed with regards to digital authentication or certification authorities. Nevertheless, central to the development of these and other standards is the public key infrastructure being developed by Canada – the Government of Canada Public Key Infrastructure (GOC PKI). Acting as a precedent, the GOC PKI is being developed to support the federal government's efforts with respect to electronic service delivery. The GOC PKI is to provide a basis for the use of digital signatures and secure internal and external electronic transactions. Currently, there are a number of government departments and agencies

⁸² *Ibid.* at 110-111.

⁸³ It was noted in the speech by the Honourable John Manley (Minister of Industry) in October of 1998 that businesses wanted “the freedom to determine their own security solutions – not have them imposed by government.” *Supra* note 28.

⁸⁴ *Supra* note 77 at 6.

actively engaged in developing this technology⁸⁵, as well as a number of departments currently using the technology on a test platform.⁸⁶

Public key infrastructures support the use of applications that encrypt data using the public key cryptography method, as well as the use of digital authentication. In short, the uses of a number of encrypted components are employed in conjunction to form a secure public key infrastructure. These infrastructures are vital to electronic commerce in that they provide security for electronic service delivery between parties who do not have a previously established relationship. Encrypting data, or affixing a digital signature, is a simple process for users, and is done automatically by clicking on an icon in a public key infrastructure enabled software package.

The establishment of any policy within a public key infrastructure is first described in a Certificate Policy document. The Certificate Policy document, which is akin to a constitution, indicates what must be done to manage the certificates in question. In essence, it is the set of rules that govern the applicability of a certificate to a particular community and/or class of applications with common security requirements. In doing so, it indicates whether or not a particular certificate is appropriate for a particular application or purpose. Each certification authority may adopt more than one policy, however, the Certificate Policy establishes in all cases the trust in each certificate.

⁸⁵ Current members of the GOC PKI are: Treasury Board Secretariat, Communications Security Establishment, Royal Canadian Mounted Police, Department of Foreign Affairs and International Trade, Department of National Defence, Citizenship and Immigration Canada, Revenue Canada, Health Canada, and Government Telecommunication and Informatics Services.

⁸⁶ It is anticipated that sometime in the year 2000 these departments will move off the test platform and onto production platforms. *Supra* note 60 at 5.

The Certification Practice Statements within public key infrastructures detail the technical aspects for achieving the policies outlined in the Certificate Policy. They are comprehensive in the sense that they detail exactly how the Certificate Policy will be implemented and maintained by each individual certification authority. Even though there is only one Certification Practice Statement in each public key infrastructure, each CA can support more than one confidentiality Certificate Policy and more than one digital signature Certificate Policy. In short, a Certificate Policy may be applied to more than a single organization, whereas a Certification Practice Statement applies only to a single CA.

The GOC PKI supports a multiple security policy domain. The Government of Canada PKI Certificate Policies assumes a need for a minimum of four digital signature certificate policies; including, rudimentary, basic, medium, and high assurance levels.⁸⁷ The details of each assurance level were documented using the Internet Engineering Task Force PKIX part 4 framework.⁸⁸ The definitions of each assurance level are as follows:

Rudimentary Assurance Digital Signature Certificate Policy – “This policy is for certificates that are to be used for low assurance authentication purposes only. It is intended for WWW client authentication with applications using SSL. At a minimum, a subscriber is authenticated by comparing presented personal information with the contents of a reference database. Certificates operating under this policy should not be relied on for document signatures. No liability will be assumed by infrastructure components.”

Basic Assurance Digital Signature Certificate Policy – “This policy is intended for the management of certificates to be used to authenticate access to information up to and

⁸⁷ Canada, *Certificate Policy: Government of Canada Public Key Infrastructure* (1999) Version 3.02, online: Treasury Board of Canada <http://www.cio-dpi.gc.ca/pki/Documents/PDF/cp_v302_2.pdf> (last accessed: 11 March 2000).

⁸⁸ See generally *Supra* note 73.

including Low-Sensitive and to establish commitments and certify performance up to a value of CAD \$5,000. A prospective subscriber must be authenticated by the CA or an LRA operating on their behalf, however this authentication does not need to be in person. No liability will be assumed by infrastructure components. For algorithms other than elliptic curve algorithms, keys must be a minimum of 1024 bits long.”

Medium Assurance Digital Signature Certificate Policy –

“This policy is intended for the management of certificates to authenticate access to information up to, and including, Particularly Sensitive and/or to establish commitments and certify performance up to a value of CAD \$50,000. A prospective subscriber must be authenticated in person by the CA or by an LRA operating on their behalf. Limited liability will be assumed by infrastructure components. Keys must be a minimum of 1024 bits long. The client application cryptographic module must be validated to FIPS PUB 140-1 level 1 or higher.”

High Assurance Digital Signature Certificate Policy –

“This policy is intended for the management of certificates to be used to authenticate access to information up to the access privilege encoded in a high integrity certificate and/or to establish commitments, certify performance and authorize settlements up to the authorized signing privilege associated with and delegated to the subscriber. A prospective subscriber must be authenticated in person by the CA or by an LRA operating on their behalf. Limited liability will be assumed by infrastructure components. Keys must be a minimum of 1024 bits long. The client application cryptographic module must be hardware (e.g. token) based and validated to FIPS PUB 140-1 level 2.”⁸⁹

The Government of Canada’s policy in implementing these assurance levels for digital signatures is to, among other objectives, encourage the development and use of open standards for commercial products that use public key cryptography.⁹⁰ In short, the Government of Canada is assuming a ‘model user’ role in developing a public key

⁸⁹ *Supra* note 71 at 14.

infrastructure whereby certain basic standards are set – both technically and in terms of policy. In part, these standards will be implemented as the GOC PKI interfaces with the private sector and international PKIs. These PKIs in turn will, to a large extent, have to adhere to similar levels of privacy, integrity, and security standards, in order to provide the easy and seamless secure electronic network demanded by Canadians.

The key lengths noted for basic, medium, and high assurance levels are strong encryption levels (128 bit) and will undoubtedly provide a maximum level of protection for users. This strong encryption level adopted by the Government of Canada will also provide, to the extent it is understood by users, a high degree of certainty. To this end, the Government of Canada has taken an initiative and addressed key length.

Nevertheless, despite the ‘importance’ the government has demonstrated in key length requirements, there remain no restrictions or requirements in the private sector on key length in order to meet a particular assurance level.

The adoption of a ‘model user’ role suggests that industry will follow the government’s lead as to the basic standards necessary for electronic commerce. In part, it suggests a *laissez-faire* ‘model user’ approach will foster innovation, and in the end, will empower end users by allowing them to choose what types of software they wish to use. There are no fears of untrustworthy CAs or inadequate software under this approach because it is assumed that government in its dealings with citizens will ensure such a large market for its products, that the standards it sets (e.g.: key lengths set for transactions) will be met by private firms because most citizens will already have the

⁹⁰ Canada, *Policy For Public Key Infrastructure Management in the Government of Canada*. (1999), online: Treasury Board of Canada <http://www.cio-dpi.gc.ca/pki/Documents/TBPolicy/method_e.html> (last accessed: 11 March 2000).

software government is endorsing. As well, this approach allows market forces to benefit Canadians because of a greater choice of technology, at lower prices.

Despite the potential benefits of the 'model user' approach, this approach is not the most appropriate means to provide security and certainty to end users. The 'model user' approach raises questions not only about the adequacy of self-regulatory frameworks, but also about the extent to which the 'model user' role will provide a safe standard. In short, the 'model user' approach will not guarantee that a uniform standard to key length and security will be followed nation wide by all small and large businesses, which is an impediment to the growth and acceptance of electronic commerce.

A recent example of the 'model user' approach taken by government is with the use of encryption in the banking industry. The banking industry is one area where encryption has become commonplace whereby banks continue to use encryption to protect I.D. numbers that customers use at bank automated teller machines (ATMs). As well, many banks encrypt the customer data on ATM cards in order to protect against forgeries. These systems use the U.S. Data Encryption Standard (DES), which arguably has reached or will soon reach the end of its useful life. The National Institute of Standards and Technology re-certified DES in 1993 but suggested that its days as an official standard are numbered.⁹¹

DES may be the most widely employed encryption algorithm and although it has been in use for over 20 years, it continues to be a commonly cited benchmark.⁹² This benchmark, however, is inadequate for electronic commerce in Cyberspace. Today, a serious effort (approximately a \$300,000 budget) by an attacker could find a DES key in

⁹¹ *Supra* note 49.

an average of 19 days using off-the-shelf technology. A business or government willing to spend more (approximately \$10 million) could expect to recover a DES key on average in 6 minutes.⁹³ The bottom line is that DES is increasingly easier to decode than many believe.

Information in Cyberspace must be kept confidential for long periods of time and therefore an assessment of encryption systems cannot be limited to what is adequate protection today. A rough estimate of the minimum strength required as a function of time can be obtained by applying an empirical rule called 'Moore's Law'.⁹⁴ 'Moore's Law' holds that the computing power available for a given cost doubles every 18 months. Taking this into account, in 1996, Blaze et al. found that a minimum key length of 90-bits was required in all commercial transactions to provide a safe level of protection.⁹⁵

Banking systems operate on closed networks and are thus less vulnerable than electronic commerce transaction via the Internet – which is an open network. The potential for more attacks on this open system leads to the assumption that better security will be required. Moreover, the need for current and 'unbreakable' encryption will be necessary. If a minimum standard is not provided uniformly throughout the nation, consumer transactions will remain vulnerable to attacks. Furthermore, unlike banking systems, attackers on an open network can easily disappear leaving the customer with no redress. However, legislation that mandated the use of certain 'safe' encryption keys would provide Canadian consumers with a higher degree of certainty in transactions.

⁹² *Supra* note 29 at 6.

⁹³ *Ibid.*

⁹⁴ *Ibid.* at 7.

⁹⁵ *Ibid.*

Another concern of the 'model user' approach is that the continued innovation and development of encryption algorithms questions the ability of smaller firms to consistently update and employ the latest and best products. To some measure, governments may be able to routinely check their systems and make sure their operations are quality, and in the best interest of consumers. However, smaller firms (e.g.: smaller banks, or vendors on-line) may not have the necessary resources or personnel to meet the government's challenge. Perhaps, in the absence of legislation, this will result in no uniform standard being met, and certainty in Canada's electronic industry will falter. If legislation mandated a minimum key length, however, the government would be responsible for reviewing the latest developments in key lengths. It would have to determine, on balance, what the most appropriate key length would have to be to ensure the protection of consumers, and then require it to be used by law.

5. AN INTERNATIONAL PERSPECTIVE ON E-COMMERCE SECURITY

This chapter illustrates the international trend to de-regulate the use and distribution of strong encrypted products. This trend is apparent partly because various governments have increasingly understood the importance of encryption in promoting electronic commerce and the personal privacy of their citizens. Although governments have yet to lift all export controls regarding cryptography, it is argued in this chapter that the trend to do so illustrates the importance of encryption products, and that the potential in the near future to require the use of strong encryption should not be discounted. The value of investigating international cryptography policy lies in the fact that 'power politics' plays a major role in the development of cryptography technology because it is considered a 'dual use' technology (e.g.: it can be used for military or commercial purposes). Moreover, an investigation of international perspectives in this area will help inform Canadian government policies.

This chapter begins with a discussion about the role of export controls. This discussion then leads to a description and analysis of the major international arrangement concerning cryptography, the Wassenaar Arrangement. The United States and United Kingdom cryptography policies will then be discussed, as these nations remain to a large extent the major players internationally in terms of economic and military power.

5.1 The Role of Export Controls

The current global situation with regard to cryptography technology is remarkably influenced by the role of export controls. Export controls are the strongest means whereby governments can restrict the use and distribution of cryptography products. By placing restrictions on these products, export controls reduce the availability of

encryption in common programs such as operating systems and electronic mail systems. In turn, these restrictions impact on the interoperability of different programs because various countries are left to develop their own programs, which often are not as secure because of a lack of peer review. Moreover, because markets for cryptography technology are made smaller by these restrictions, companies and individuals are not as interested in developing programs because of smaller potential profits.

Some countries have taken advantage of this situation. Switzerland, for example, notes that it wants to keep an “efficient export permit for cryptography” in order to increase sales worldwide, while at the same time being mindful of national security issues.⁹⁶ As well, Canada in its recent pronouncements on cryptography noted that it wants to “allow Canadian producers to export their products globally within the framework of international arrangements”.⁹⁷ Other countries, however, have been reluctant to loosen export controls and as a result have seen their cryptography firms move to countries that have no restrictions. This is especially true with American companies who have increasingly moved their encryption production divisions overseas to countries with fewer controls, such as Switzerland.⁹⁸

This increased globalization of firms warrants the following brief international survey on cryptography technology. It is warranted because of the significance interoperability has on electronic commerce security. To the extent that encryption will foster e-commerce trading on-line, and to the extent that it will foster consumerism, there

⁹⁶ Electronic Privacy Information Centre, “Cryptography and Liberty 1999: An International Survey of Encryption Policy, Electronic Privacy” (1999), online: EPIC <<http://www.gilc.org/crypto/crypto-survey-99.html>> (last accessed: 11 March 2000).

⁹⁷ *Supra* note 28.

⁹⁸ *Ibid.*

is an increased need for not only uniform global encryption standards, but also the general use and distribution of encryption products. If countries restrict the use or distribution of this technology, the necessary uniform standards and general use of encryption products will be not be cultivated. Consequently, to some measure e-commerce security depends on the international acceptance of encryption.

Globalization (more specifically globalized politics) inherently impacts as well on the acceptance of encryption. In short, the role of various governments in influencing other government actions can have a potentially serious impact in that; 'power politics' may play a significant role.⁹⁹ As a result, an international perspective on cryptography technology will help illustrate the extent to which larger, and more influential nations, are imposing their fears and opinions on other nations who do not have the same fears of, or aspirations for, cryptography.

Most of the fears regarding cryptography technology come from the fact that it allows for secret communications. Accordingly, some governments have restricted its use on the basis of national security issues. In essence, certain governments have regarded cryptography as an impediment to law enforcement agencies to such a degree that they fear terrorists could easily conspire and compromise the government using cryptography in such a way that it would give law enforcement agencies no way of defending themselves or their citizens.

This fear became so rampant, especially in the United States, that export controls on cryptography were designed to keep all cryptography products (even the algorithms) within the country. Nevertheless, the U.S. government has recently retreated from some

⁹⁹ See analysis by Held and McGrew chapter 2.

of its severe export controls. To a large measure the U.S.'s willingness (as well as Canada's and the United Kingdom's) to cautiously remove restrictions (or at least not to add any new restrictions) on the use and export of encryption are shaping recent international developments.

5.2 The Wassenaar Arrangement

On December 19, 1995, a group of 33 industrial nations reached a formal arrangement to restrict the export of conventional weapons and 'dual use' technology to certain 'pariah' states, or states that were currently at war. The Wassenaar Arrangement (WA) restricted several cryptography products, along with other technologies such as supercomputers and high-level computer security access software, which were all considered under this arrangement to be 'dual use' products in that they could be used for both commercial and military purposes.

The Wassenaar Arrangement is the successor to the Cold War-era Coordinating Committee on Multilateral Export Controls (COCOM), a group of 17 nations that placed restrictions on the export of certain technology to countries of the former Warsaw Pact and other communist states. The WA is open on a global basis provided that other countries comply with the export control criteria. To this end, an outreach policy is being planned to inform non-member countries about WA objectives and activities and encourage non-member countries to adopt the WA national policies on the export of conventional arms and 'dual use' technologies (including cryptography).¹⁰⁰

The WA is neither an international treaty nor a law. Its purpose is to exchange views and information on international trade in conventional arms and 'dual use'

¹⁰⁰ *Supra* note 96.

products. As a result, all participating states committed to the arrangement pledge to adjust their national export control policies to adhere to the WA control lists. As this arrangement is not a treaty or law, participating states may adjust their cryptographic export policies through new domestic regulations or legislation.

The WA represents the interests of law enforcement, intelligence, and weapons control sectors of each participating government. As such, little regard is directed to commercial concerns regarding each technology. Still, the WA maintains that restrictions are not directed at impeding the development of commerce, or any particular state. Each participating country however has the ability to construct national sanctions, and each nation's sanctions accordingly vary widely. These substantial disparities between participating countries are important disadvantages in the application of uniform WA export control measures.

On December 3, 1998, the Wassenaar Arrangement Secretariat announced new cryptography guidelines. In part, it extended the control list to include encryption hardware and software products above 56-bits. These new restrictions obligated each participating country to establish new export controls over 'mass market' encryption software that use keys longer than 56-bits. As well, countries that adopt the Wassenaar Arrangement also now agree to control software used for specific sectors such as banking, insurance, and health. According to the new control list, all of these software packages are to be kept under 56-bits.¹⁰¹

¹⁰¹ *Ibid.* This restriction only applies to certain countries. For example the U.S. policy indicates they can export products with a licence over 56-bits to these specific sectors in 45 different countries.

What constitutes an important loophole in the latest amendments to the Wassenaar control list, is that the controls do not apply to the 'intangible' distribution of cryptography, including downloads from the Internet.¹⁰² Therefore, it remains to be seen what effects these new provisions will have on the flow of encryption products, particularly now that Canada and Switzerland (and Germany) have indicated that they do not plan to impose new strict restrictions on the exports of encryption software.¹⁰³

These recent arrangements endorsed by Wassenaar clearly indicated that key size is an issue at the international level. To the extent it is an issue, however, there is a realization that strong encrypted products are being regulated, but in the sense that their use is controlled and/or regulated by a license – at least internationally. This is certainly an important consideration in implementing domestic technical requirements for e-commerce security, as interoperability will play a significant role in Canada's ability to participate in the new global economy.

Coming to some conclusion as to why restrictions are being placed on encryption products that use keys over 56-bits may require speculation. Then again, a look at some of the more powerful nations (powerful in terms of political, economic, and military power) and those nations that have high connectivity rates to the Internet, reveals that most of the international debates and concerns about cryptography technology have been misguided up until recently. In short, discussions around cryptography have been focused on criminal and national security issues. To some measure, cryptography policies surrounding the protection of consumers' interests, general democracy, and the overall promotion of electronic commerce have been overlooked. However, as countries

¹⁰² *Ibid.*

begin to realize the importance of e-commerce and electronic privacy, they seem to be slowly relieving export controls and strict regulations on the use and distribution of cryptography products.

5.3 The United States

Prior to 1998, the United States government restricted the export of encryption products over 40-bits. The agencies responsible for regulating cryptography products at the time considered strong encryption to be systems that used RSA with key sizes over 512-bits, or symmetric algorithms (like DES, IDEA, or RC5) with key sizes over 40-bits. Since government encryption policy was heavily influenced by the agencies responsible for gathering domestic and international intelligence (the FBI and NSA) the government was compelled (and to some measure is still compelled) to balance the conflicting requirements of making strong cryptography available for commercial purposes, while at the same time still making it possible for those agencies to have access to encrypted data. The U.S. government did, however, allow 56-bit block ciphers to be exported for financial cryptography.

The government's regulation of cryptography products was, and still is, highly debated. Three cases were brought before U.S. courts between 1996 and 1997 to challenge the government's position on the export controls of cryptography. The principal arguments that these cases made were: the regulations set by the government were unconstitutional prior restraints on speech under the First Amendment; they violated the plaintiffs' rights to due process under the Fifth Amendment; and the International Emergency Economic Powers Act (IEEPA) did not authorize them.

¹⁰³ *Ibid.*

Bernstein v. United States Department of State is the leading case.¹⁰⁴ The plaintiff, Bernstein, developed a specialized cryptographic algorithm and sought to export the source code and an academic paper discussing the algorithm. The U.S. government denied Bernstein the ability to export the algorithm, however, under its export laws. Bernstein claimed that these regulations prevented him from discussing his work at public meetings and from publishing the work. As a result, he asserted he was unable to advance his professional reputation and career by publishing and discussing his work with professional peers and others.

In the first Bernstein decision, Judge Patel held that cryptographic source code was speech protected by the First Amendment and that Bernstein's claims were justifiable.¹⁰⁵ In a second decision, Judge Patel held that encryption licensing schemes were a prior restraint under the First Amendment, and thus held in favor of Bernstein once again.¹⁰⁶ On a third issue, however, Judge Patel ruled in favor of the government on the statutory challenges under IEEPA, but held that the encryption export regulations were unconstitutional as a prior restraint on protected speech.¹⁰⁷ Upon appeal, a Ninth Circuit court ruled that the export regulations were in fact unconstitutional and affirmed the district court's decision in the third Bernstein case.¹⁰⁸

The Bernstein case was a major victory for the First Amendment in the computer age. It confirmed that the use of specialized tools to speak, like a computer, or a specialized language to communicate, like a programming language, do not put people

¹⁰⁴ *Bernstein v. United States Department of State*, 922 F.Supp. 1426 (N.D. Cal. 1996).

¹⁰⁵ *Ibid.*

¹⁰⁶ *Bernstein v. United States Department of State*, 945 F. Supp. 1279 (N.D. Cal. 1996).

¹⁰⁷ *Bernstein v. United States Department of State*, 974 F. Supp. 1288 (N.D. Cal. 1997).

¹⁰⁸ *Bernstein v. United States Department of Justice*, 192 F.3d 1308 (9th Cir. 1999).

outside the scope of the First Amendment. In short, this decision announced that the U.S. Government unconstitutionally prevented the export of cryptographic source code with a system of speech licenses. As Michael Froomkin notes, this decision also marked an open admission by the U.S. government that it had been using the export control laws to retard the domestic use of cryptographic software.¹⁰⁹

Before the Ninth Circuit court ruled on Bernstein's case, the U.S. government announced updates to the Administration's encryption policy. This announcement indicated the government's intention to expand its encryption policies to serve a full range of national interests including promoting electronic commerce, supporting law enforcement and national security, and protecting privacy. As well, the announcements permitted the export of strong encryption to protect sensitive information in the financial, health, medical, and electronic commerce sectors. The government also eliminated key recovery commitment plans, and allowed any source code regardless of key length) to be eligible for export under a license exception to U.S. subsidiaries for internal company proprietary use.¹¹⁰

Furthermore, under the new encryption policy, encryption commodities including mass market and non-mass market software incorporating symmetric algorithms with lengths up to and including 56-bits were authorized for license exception to all destinations except Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria. Nevertheless, encryption chips, integrated circuits, toolkits, and executable modules are not authorized

¹⁰⁹ Michael Froomkin, "Statement on the Bernstein Case" (1999), online: Michael Froomkin's Homepage <<http://www.law.miami.edu/~froomkin/bernstein99.htm>> (last accessed: 11 March 2000).

¹¹⁰ License exceptions can be granted for all countries except Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria. *Supra* note 96.

for export under license exception. In terms of electronic commerce, the U.S. encryption policy authorized encryption commodities and software of any key length for on-line merchants in 45 countries. Such commodities, however, are limited to client-server applications, or applications specifically designed for on-line transactions (e.g.: no other end-uses or customer to customer communications or transactions are allowed)¹¹¹

One year after these announcements, the U.S. government declared a new approach to encryption policy.¹¹² In September of 1999, the government updated its guidelines to allow U.S. companies new opportunities to sell their products to most end users in global markets. Under the new policy, any encryption commodity or software of any key length may be exported under license exception after a technical review. Further, any retail encryption commodities and software of any key length may be exported under license exception. Both of these export license exceptions however are only valid if they are being exported to any country but the 'seven state supporters of terrorism'. Under these new guidelines streamlined post-export reporting was adopted to provide government with an understanding of where strong encryption is being exported. Finally, sector definitions and country lists were eliminated.

The developments that have been made in the past four years in the United States regarding cryptography technology illustrates a trend to move away from severe export controls on strong encryption. In addition, there has been a realization by the U.S. government that cryptography technology is a vital technology that will help enable the

¹¹¹ *Ibid.*

¹¹² Statement by the Press Secretary, "Administration Announces New Approach to Encryption" (September, 1999), online: Center for Democracy and Technology <<http://www.cdt.org/crypto/CESA/whousepress091699.shtml>> (last accessed: 3 April 2000).

new global economy. As the trend is to de-regulate the restrictions on strong encrypted products, it is no surprise that mandated strong encryption legislation has not been debated or even considered. Nevertheless, the trend by the U.S. government to de-regulate the use of strong encrypted products lends credibility to the importance of key length in securing electronic commerce transactions. As the U.S. government has made significant compromises over the past few years, and has moved towards less severe export controls to help promote domestic and foreign use of strong encryption, the possibility of mandating the use of strong encryption products in the future should not be over-looked.

This may be the case as stronger and more influential nations, such as the United States, who have a large impact internationally (both in terms of 'power politics' and such arrangements as Wassenaar) continue to place more and more importance on the use of strong encryption to protect their citizens from fraud in electronic transactions. Moreover, e-commerce could conceivably come to a point that the mere availability of these products is insufficient in protecting consumers. There may come a time when electronic transactions are mainstream and domestic economies rely so heavily on e-commerce, that protecting transactions on-line will necessitate the strongest encrypted software. In short, there will come a time when e-commerce security will be considered so vital to the survival of the nation that it can not be left to the private sector – partly because it may not be assured by the private sector.

5.4 The United Kingdom

The U.K. has been the strongest supporter of the United State's efforts to promote key escrow and general limitations on encryption. Although there remain no domestic use

restrictions, or restrictions on the import of cryptography into the U.K., to some measure it has always shown interest in regulating the export of cryptography. To this end, some of its proposals have not been in line with the rest of the European nations.

In 1996 the U.K. government conducted public consultations on the regulation of trusted third parties (TTPs). By March of 1997, legislation on the licensing of TTPs for the provision of encryption services was released. The Department of Trade and Industry in 1998 detailed the government's position at the time by indicating the intention to introduce legislation to license TTPs and certification authorities. Although these requirements were voluntary (as was requested by industry) the government strongly encouraged organizations to use these standards in order to provide confidence in electronic commerce.

In March of 1999, pending the "Secure Electronic Commerce Bill", the Prime Minister met with industry representatives and announced that the government was 'backing away' from support for the linking of licensing with escrow requirements.¹¹³ The government announced that it wanted to examine alternatives to escrow encryption that would help assist law enforcement agencies. In the end, they suggested that escrow encryption would not be fully discounted, and that if sufficient alternatives were not produced, the government would then adopt the escrow encryption method.¹¹⁴

A report by the Cabinet Office in May of 1999 entitled *Encryption and Law Enforcement* furthered the government's stance on escrow encryption.¹¹⁵ Within this

¹¹³ *Supra* note 96.

¹¹⁴ *Ibid.*

¹¹⁵ United Kingdom, "Encryption and Law Enforcement" (1999), online: Cabinet Office <<http://www.cabinet-office.gov.uk/Innovation/1999/encryption/index.htm>> (last accessed: 11 March 2000).

report, the U.K. government made recommendations that suggested key escrow should not be mandatory and that there should be a new approach based on cooperation with industry. The Task Force further welcomed the intention to include in the forthcoming Electronic Commerce Bill provisions to allow lawful access to decryption keys and/or plain text under proper authority. Also, they recommended that further attention should be given in the Bill to placing the onus on the recipient of a disclosure notice to prove to the authorities that the requested keys are not in their possession.

The intent of the new encryption policy was met by criticism. A critical letter on the new encryption policy was sent to the Prime Minister on behalf of the U.K. organization Cyber-Rights & Cyber Liberties.¹¹⁶ The letter advised the government that the absence of any coverage on cryptography export controls and their detrimental impact on electronic commerce was a surprising and serious omission. Further, it was remarked that it would be a grave embarrassment, both for the Government and for Britain's position in the world of electronic commerce, for the Government's E-Commerce Bill to be found inconsistent with the Human Rights Act.

On November 17, 1999, two new Bills were introduced that related to encryption and electronic commerce. The first Bill was the "Electronic Communications Bill" and it permitted Internet users to sign messages electronically. Further, it introduced a 'kitemark' for minimum standards of quality and service. The second Bill brought the U.K. into line with Europe by strengthening the regulation of covert surveillance. The "Regulation of Investigatory Powers" Bill provided for lawful access to encrypted data. The government maintained that this was the alternative it found to escrow encryption in

that this Bill would regulate techniques which are necessary for the protection of society at large but which can impact on the privacy of individuals. As a result, the government was satisfied that this Bill would strike a balance between these aims in accordance with the obligations under the European Convention on Human Rights.

Notwithstanding the governments revised stance on escrow encryption (which is quite strong because under section 13 of the new Electronic Communications Bill there is a 'prohibition on key escrow requirements') the U.K. government still maintains export controls on cryptography pursuant to its participation in the Wassenaar Arrangement. Moreover, the U.K. strongly supported the amendments to the Wassenaar dual-use control list announced in December 1998 – e.g.: to lift the exportable key size to 56-bits. In fact, it has recently taken steps to further the restrictions on cryptography placed by the WA. The U.K. intends to extend export controls beyond tangible cryptography to intangible exports of encryption products – e.g.: cryptography that could be downloaded from the Internet.¹¹⁷

The Department of Trade and Industry is responsible for issuing export licenses for encryption. Nevertheless, firms wishing to obtain a license must also send their applications to the Communications and Electronic Security Group – the equivalent to the Communications Security Establishment in Canada. In practice, the Department of Trade and Industry usually follows the recommendations by the Communications and

¹¹⁶ This letter can be found at the Cyber-Rights & Cyber-Liberties (UK) web site: <http://www.cyber-rights.org/reports/blair-letter.htm> (last accessed: 11 March 2000).

¹¹⁷ *Supra* note 96.

Electronic Security Group.¹¹⁸ In short, the current procedure for export licenses is clearly under the control of a United Kingdom security agency.

Although the U.K. government continues to maintain tighter export controls on cryptography technology than the U.S. and Canada, it has made concessions to their encryption policy; namely in the area of escrow encryption. To this regard, it is conceivable in the near future that the government will address its export control laws partly because there continues to be a great deal of attention on the issue. Export controls laws are coming more and more under attack by privacy and civil liberty associations because citizens and businesses are demanding the freedom to use cryptography. As the larger and more powerful nations, such as the U.K., realize that cryptography export regulations are important to their economy and instill trust in their citizens, it seems there will continue to be more and more concessions made – such as the concession ‘demanded’ by business with regards to escrow encryption.

Further, as countries such as the United States and Canada continue to allow strong encrypted products to be exported, the U.K. will more than likely have to follow suit. Not doing so would present interoperability problems for U.K. electronic commerce. The Bernstein case in the United States also, to some measure, sets an international precedent in the sense that if export control laws can be found unconstitutional in the United Kingdom, the market for strong encrypted products will flourish. Accordingly, the Bernstein case could mark the beginning of a ‘mass-market’ for strong encryption products. This proliferation of strong encryption will essentially place more importance on its use in electronic commerce. If this is the case, then

¹¹⁸ *Ibid.*

countries such as Canada should not over-look the next precedent regarding cryptography and electronic commerce security; that being the mandating of strong encryption software to provide trust, security, and certainty in the new global electronic economy.

6. CONCLUSIONS

The intention of the final assessment is to illustrate the role of international organizations and the continued importance and role of the Canadian government in implementing cryptography standards. In the end it is suggested that minimum key length requirements be mandated at the international and national levels in order to provide a high degree of certainty in transactions, as well as to protect consumer interests. Further, it is recommended that the Canadian government maintain standards in this area in order to foster national sovereignty and democracy in cryptography and electronic commerce.

6.1 The Role of International Organizations

International organizations such as the WTO, UNCITRAL, OECD, UNCTAD¹¹⁹, and the ICC¹²⁰ are actively involved in discussions with governments and businesses to address key legal issues raised by the emergence of a global marketplace. These on-going efforts will undoubtedly help establish a secure electronic commerce infrastructure for the 21st century that, once in place, will contribute to the building of the necessary legal framework and the necessary level of trust required for e-commerce development.

The need for international uniform rules and technical standards in the area of electronic commerce is of paramount importance. In order to create a seamless transition into the electronic global economy Canada must remain active at the international level. In doing so, Canada must be involved in representing its views on international treaties and agreements regarding electronic commerce. If Canada does not aggressively partake in international negotiations it could build trade barriers between Canadian firms and

¹¹⁹ United Nations Conference on Trade and Development.

¹²⁰ Internet Chamber of Commerce.

international firms. In short, Canada's economy will suffer if it does not align its national economic policies and legal frameworks with international arrangements.

In establishing a firm electronic commerce infrastructure it seems clear that key length standards must be addressed. While some may decry that setting an international technical standard will hamper innovation by biasing a certain technology, setting a specific minimum key length is not technologically biased, and in the end will not hamper innovation. The promotion of a uniform encryption minimum standard will not mandate a specific software package, but rather, a specific level of security. In the end, this security level will have a positive impact on electronic commerce as a whole.

As encryption continues to be recognized as an important device for electronic commerce, international organizations should develop technical standards that require a uniform minimum level of security in all electronic transactions. In doing so, it will undeniably create a high level of certainty in all transactions on-line. If this standard is not set, however, the necessary level of trust, and to some measure, the necessary interoperability, will not be achieved. Minimum key length is the one component that governments can proscribe that will help provide a solid foundation for the global marketplace, yet at the same time allow for innovation.

The role of international organizations must be recognized as an important beginning for technical standards. International forums should inaugurate a key length standard first by voluntary code. A voluntary code would not bind countries to mandate a minimum key length. As well, a voluntary code may make sense to begin partly because certain levels of encryption technology (e.g.: strong encryption) are still not available in some countries. Nevertheless, a voluntary code would at the very least begin the process

of uniformity. As electronic transactions increase, and the level of international electronic transactions increases, the voluntary code could later be formalized as a treaty. At this time, countries will have developed a more sophisticated electronic infrastructure and will be more likely to sign a binding treaty.

As strong encryption (e.g.: 128-bit) is still 'unbreakable' it is the first level of encryption that international organizations should be discussing. This level of encryption will create an unparalleled level of security that will ensure certainty in all transactions. Nevertheless, it is suggested that the job of international treaties and agreements in setting a security standard is to monitor the development of cryptography. Therefore, although 128-bit encryption is currently a standard that could be set to reasonably engender confidence in transactions now, the on-going role of any international treaty would be to up the standard once technology advanced to the point where the key length mandated is vulnerable (e.g.: it can be hacked into).

It is by mandating a minimum encryption standard that consumer interests will be protected. In short, if strong minimum encryption standards were consistently mandated, consumers could reasonably assume that the information they send into Cyberspace will be protected from those parties for whom it is not intended. It is suggested that this is one reason (the protection of consumers) that an international treaty should mandate these standards. If consumers cannot be confident that their transactions on-line will be protected, then global electronic commerce transactions will not have the impact or the benefits that many are predicting, and as a result, many businesses and local economies will suffer.

6.2 The Role of the Canadian Government

While the Canadian government must remain active in the development of cryptography technologies at the international level, it must also prepare national policies regarding this technology. The continued role of the Canadian government in setting international policies, therefore, must be recognized as only one component of the larger regulatory agenda it must confront regarding cryptography and electronic commerce. In short, the Canadian government's role in setting uniform standards within Canada will influence how the local economy is directed.

If Canada does become a signatory to an international treaty that stipulates specific encryption requirements it does not automatically bind all Canadians to use those standards. Although treaties are important sources of international law obligations, treaties that alter Canadian law, affect individual rights, or extend existing governmental powers, must be implemented in legislation within Canada. Hence, the legislature and executive must participate in the Canadian treaty making process.

While the specifics of the treaty signed will dictate if a Canadian citizen's domestic transactions are bound to use the standards set by the treaty, Canada should be prepared in the absence of international requirements to pass its own legislation to require all Canadians to use a uniform standard for domestic purposes. By creating a uniform standard in Canada, the Canadian government will protect consumers' transactions from those for whom it is not intended. More to the point, a uniform 'safe' standard will help protect consumers from business that may not update their software; it will protect those consumers with little or no knowledge of cryptography and its applications; and it will protect consumers from hackers who will exploit out-dated software. Perhaps, as well,

10 years from now it will protect the very essence of the Canadian economy – electronic transactions.

It is recognized that one of the limitations of implementing an encryption standard within Canada may be the constitutionality of a uniform standard. In short, as contractual issues are provincial domain, and communication regulations are in the federal domain, there are potentially serious constitutional implications. As well, at least theoretically, if encryption standards fell under provincial jurisdiction, Canada could end up with a mix of standards if one or more provincial governments decided to introduce a minimum key length standard. While the constitutionality of mandating a minimum key length is outside the scope of this work, it is one issue that will have to be examined before domestic regulations are enacted.

Nevertheless, the importance placed on digital authentication, the role of certification authorities, and the implementation of public key infrastructures in general by the Canadian government will play a significant role in the future of electronic commerce in Canada. International organizations, domestic governments, and provincial governments have recognized that the potential benefits of an electronic delivery infrastructure weigh greatly upon how the implementation of these technologies will be handled. To this end, government should mandate (e.g.: regulate) a minimum encryption level for all electronic transactions – this will help create certainty and trust in the electronic marketplace.

Appendix

Background on the Development of the Internet in Canada

The Internet is a technology without precedent partly because it was not invented so much as it was imagined. The Internet began in the 1960s as a United States Department of Defense's Advance Research Projects Agency (ARPA) initiative to establish a communications network between universities and the military – the ARPANet. By the mid 1980s, the National Science Foundation, using the same protocols, established its own research and academic network – the NSFNet. By the late 1980s, several for-profit organizations sought access to these networks and so transformed the once experimental technology into a commercially viable network.

The Internet is a loose association of thousands of networks and millions of computers across the world that all work together to share information. The Internet has no central or physical location, thus making all of its stored information and intelligence widely distributed. The Internet's early developers were committed to developing an open network. As a result, the Internet allows computers and networks to communicate openly and effectively. They do so by using TCP/IP (Transmission Control Protocol/Internet Protocol), the language of computer communication. As this protocol is now widely and publicly available, information freely transmits over networks and exchanges among the various networks worldwide. E-mail, file transfers, and web browsing are just a few of the services that have been realized by the use of TCP/IP.

Canada was at the forefront of Internet technology, and in the 1980s several education and research computer networks, including CDNNET, became operational in

Canada. As well, Canada's first national network, NetNorth, began operations in 1985. By 1988, a group of Canada's leading universities and research institutions together with the federal government decided to create a national computer communications network. This network connected regional networks and individual computer systems in Canada to the Internet. In June of 1990, this newly formed backbone (CA*net) was Canada's first national backbone network. Although CA*net did not own transmission facilities, it obtained high capacity digital facilities from Canada's telecommunications common carriers.¹²¹

By the early 1990s, the regional networks in all ten provinces were interconnected. The regional networks (NLnet in Newfoundland, NSTN in Nova Scotia, PEInet in Prince Edward Island, NBnet in New Brunswick, RISQ in Quebec, ONet in Ontario, MBnet in Manitoba, Sask#net in Saskatchewan, ARnet in Alberta and BCnet in British Columbia) formed CA*net's Board of Directors and directly influenced its growth and management policy formation.¹²²

Until 1992, the speed of CA*net was limited to 56 Kbps. The increase in use of the Internet in the early nineties, however, precipitated a need to upgrade the speed of CA*net to handle the increase in traffic. As a result, in January 1993, the Canadian government announced a government-industry initiative designed to encourage industrial research and development into high-bandwidth network facilities and applications. This initiative established the Canadian Network for the Advancement of Research, Industry and Education (CANARIE). The first objective of CANARIE was to upgrade CA*net to

¹²¹ Catherine Peters, "The Internet in Canada" (1997), online: Industry Canada <<http://strategis.ic.gc.ca/SSG/it03898e.html>> (last accessed: 17 March 2000).

¹²² *Ibid.*

T-1 or 1.5 Mbps speed and also to connect Canada's North. In the early nineties CANARIE helped establish regional networks in the Northwest Territories and the Yukon and connected them to the national backbone. Finally, CANARIE established a high-speed (T-3) experimental test bed network of ATM switches in all the regions of Canada. In CANARIE's second set of objectives, the CANARIE/CA*net backbone was upgraded to provide suitable performance under conditions of rapid growth in user demand.¹²³

Canada developed CA*net II network in 1997 which is dedicated to universities and research institutions for advanced networking services, such as university courses. The network is state-of-the-art with a capacity of 155 Mbps or more on fiber optic wiring. It guarantees bandwidth and allows developments that were not possible because of the congestion problems of the broader public network.¹²⁴ This new network and the commercial networks use common facilities and will essentially provide the new generation of Internet users with unprecedented capabilities.

Electronic Commerce and Cryptography

Electronic commerce has been growing steadily throughout the 1980s and 1990s, but it was not until the mid 1990s that commercial activity was taking place on public and open networks like the Internet. Most of the e-commerce transactions before the mid 1990s were business-to-business transactions involving large manufacturers in industries such as auto and retail merchandise, and simply involved placing orders with their suppliers. Electronic payment systems were also established (such as the debit card system) that operated on a closed network. Many government agencies also disseminated

¹²³ *Ibid.*

procurement notices and accepted bids from vendors through these 'value-added networks'.

In 1994, a number of fee-based information services began operations on the World Wide Web. Soon after, companies began selling consumer and industrial goods as well as providing intermediary services such as obtaining quotes for insurance coverage. As well, access to pornography played a large role in the early development of e-commerce transactions. By 1997, the total value of electronic commerce conducted on the Internet was estimated at 8 billion dollars U.S. per year.¹²⁵ Recent revenue projections indicate that by 2002, electronic transactions on the Internet will total 400 billion dollars U.S. per year.¹²⁶ These figures are still modest in comparison to transactions elsewhere, yet, with the skyrocketing growth in Internet users (it is predicted that as many as 100 million consumers will be on-line by 2001 in the United States alone¹²⁷), electronic commerce will undoubtedly play a more significant role in the economy.

As electronic transactions on the Internet become mainstream there is a need to protect the information being transferred. In doing so, cryptography technology is now being used to disguise data. Cryptography as a science has existed for thousands of years and may be summed up as the study of techniques and applications that depend on the existence of difficult problems. In its simplest form, however, cryptography is concerned with keeping communications private. Indeed, the protection of sensitive

¹²⁴ *Ibid.*

¹²⁵ United Nations Conference on Trade and Development, *Policy Issues Relating to Access to Participation in Electronic Commerce* 1998 UN Doc. TD/B/COM.3/16 at 4.

¹²⁶ *Ibid.* at 4.

¹²⁷ *Supra* note 37.

communications has been the emphasis of cryptography throughout much of its history. Nevertheless this is only one part of today's cryptography.

Traditionally, cryptography was the almost exclusive preserve of governments. Cryptography was used to protect military or diplomatic secrets and was predominantly embedded in the hardware. Today's advancements in encryption technology have led to some profound changes in our everyday lives, however. Encryption technology is now used for authentication throughout our daily routine.

The use and importance of cryptography technology in facilitating the growth and security of electronic commerce is a result of the use of encryption/decryption and digital signatures. Encryption provides for confidentiality by protecting information from unauthorized disclosure or viewing by mathematically scrambling the original text. Digital signatures, however, provide three basic attributes. First, digital signatures provide a means for authentication. Fundamentally this includes proof that users are who they claim to be or that resources (e.g.: computer devices, software or data) are what they purport to be. Second, digital signatures allow for non-repudiation. This function includes proof that the transaction occurred or that a message was sent or received, thus one of the parties to the exchange cannot deny that the exchange occurred. Finally, they inject some form of integrity into electronic transactions so that data cannot be modified without detection.

Bibliography

- Abelson, Hal et al. "The Risks of Key Recovery, Key Escrow, and Trusted Third Party Encryption" (1998), online: CDT Encryption Issues Page
<<http://www.cdt.org/crypto/risks98/>> (last modified: 30 July 1998).
- Akdeniz, Yaman et al. "Cryptography and Liberty: Can the Trusted Third Parties be Trusted? A Critique of the Recent UK Proposals" (1997) *Journal of Information, Law and Technology*, online: JILT
<http://elj.warwick.ac.uk/jilt/cryptog/97_2akdz/> (last modified: 27 June 1997).
- Akdeniz, Yaman. "No Chance for Key Recovery: Encryption and International Principles of Human and Political Rights" (1998), online: Web Journal of Current Legal Issues Ltd. <<http://webjcli.ncl.ac.uk/1998/issue1/akdeniz1.html>> (last accessed: 3 April 2000).
- Akdeniz, Yaman. "UK Government Policy on Encryption" (1997), online: Web Journal of Current Legal Issues Ltd. <<http://webjcli.ncl.ac.uk/1997/issue1/akdeniz1.html>> (last accessed: 3 April 2000).
- Avineri, S. *Hegel's Theory of the Modern State* (London: Cambridge U. P., 1972).
- Bamford, James. *The Puzzle Palace: A Report on America's Most Secret Agency* (Boston: Mifflin, 1982).
- Bernstein v. United States Department of State*, 922 F.Supp. 1426 (N.D. Cal. 1996).
- Bernstein v. United States Department of State*, 945 F. Supp. 1279 (N.D. Cal. 1996).
- Bernstein v. United States Department of State*, 974 F. Supp. 1288 (N.D. Cal. 1997).
- Bernstein v. United States Department of Justice*, 192 F.3d 1308 (9th Cir. 1999).
- Bill C-6 *Information Protection and Electronic Documents Act*, 2nd Sess., 36th Parliament, Canada, 1999.
- Blaze, Matt et al. "Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security" (1996), online: Counterpane Internet Security Inc.
<<http://www.counterpane.com/keylength.html>> (last accessed: 3 April 2000).
- Canada. *Certificate Policy: Government of Canada Public Key Infrastructure* (1999) Version 3.02, online: Treasury Board of Canada <http://www.cio-dpi.gc.ca/pki/Documents/PDF/cp_v302_2.pdf> (last accessed: 11 March 2000).

- Canada. *Policy For Public Key Infrastructure Management in the Government of Canada*. (1999), online: Treasury Board of Canada <http://www.cio-dpi.gc.ca/pki/Documents/TBPolicy/method_e.html> (last accessed: 11 March 2000).
- Canada. "Report of Canadian Delegation on the Thirty-fourth Session of the UNCITRAL Working Group on Electronic Commerce" (1999), online: Department of Justice Canada <<http://canada.justice.gc.ca/en/ps/ec/un99gau.html>> (last accessed: 11 March 2000).
- Cerny, Philip G. "Globalization and the Erosion of Democracy" (1999) 36 *European Journal of Political Research* 1.
- Denning, Dorothy E. "The Future of Cryptography" in Brian D. Loader ed., *The Governance of Cyberspace* (London: Routledge, 1997).
- Denning, Dorothy E. "Resolving the Encryption Dilemma: The Case for Clipper" (July 1995), online: The Cryptography Project <<http://www.techreview.com/articles/july95/Denning.html>> (last accessed: 11 March 2000).
- Dietrich, Dale A. "Legal Issues Affecting Canadian Based Electronic Commerce Undertakings" (1998) IT Industry Series on Intellectual Property Centre for Property Studies, New Brunswick, online: SmithLyons <<http://www.SmithLyons.ca/it/ecom>> (last accessed: 11 March 2000).
- Economic Council of Canada. *Responsible Regulation: An Interim Report* (Ottawa: Supply and Services Canada, 1979).
- Electronic Privacy Information Centre. "Cryptography and Liberty 1999: An International Survey of Encryption Policy, Electronic Privacy" (1999), online: EPIC <<http://www.gilc.org/crypto/crypto-survey-99.html>> (last accessed: 11 March 2000).
- Friedmann, W. *The State and the Rule of Law in a Mixed Economy* (London: Steven and Sons, 1971).
- Froomkin, Michael. "The Essential Role of Trusted Third Parties in Electronic Commerce" (1996) 75 *Oregon Law Review* 49.
- Froomkin, Michael & DeLong, B. "Speculative Microeconomics for Tomorrow's Economy" (1999), online: University of Miami Law School <<http://personal.law.miami.edu/~froomkin/articles/spec.htm>> (last modified: November 1999).

- Froomkin, Michael. "The Metaphor is the Key: Cryptography, The Clipper Chip, and the Constitution" (1995) 143 *U. Penn. L. Rev.* 709, online: Michael Froomkin's Homepage <<http://www.law.miami.edu/~froomkin/articles/clipper.htm>> (last accessed: 11 March 2000).
- Froomkin, Michael. "Statement on the Bernstein Case" (1999), online: Michael Froomkin's Homepage <<http://www.law.miami.edu/~froomkin/bernstein99.htm>> (last accessed: 11 March 2000).
- Greer, Allan & Radforth, Ian. *Colonial Leviathan: State Formation in Mid-Nineteenth-Century Canada* (Toronto: University of Toronto Press, 1992).
- Hart, Michael. "What's Next: Negotiating Rules for a Global Economy" Occasional Papers in International Trade Law and Policy, No. 36 (Ottawa: Centre for Trade Policy and Law, 1995).
- Held, David and McGrew, Anthony. "Globalization and the Liberal Democratic State" (1994) 28 *Government and Opposition* 261.
- Held, David. "Democracy and Globalization" (1997) 3 *Global Governance* 251.
- Honorable John Manley's (Minister of Industry) speech on October 1, 1998, online: Task Force on Electronic Commerce <<http://e-com.ic.gc.ca/english/speeches/42d3.htm>> (last accessed: 11 March 2000).
- Industry Canada. *Electronic Authentication Policy Workshop Working Paper* (Ottawa, November 22, 1999).
- Internet Engineering Task Force PKIX. *Certificate Policy and Certification Practice Framework Part 4*, online: IETF Homepage <<http://www.ietf.org>> (last access: 11 March 2000).
- Mason, E. eds. *The Corporation in Modern Society* (Cambridge: Harvard U.P., 1960).
- Marx, K. *Marx: Early Political Writings* (Cambridge: Cambridge University Press, 1994).
- OECD. *Business-to-Consumer Electronic Commerce Survey of Status and Issues*, 1997.
- OECD. *Global Information Infrastructure – Global Information Society*, 1997.
- Peters, Catherine. "The Internet in Canada" (1997), online: Industry Canada <<http://strategis.ic.gc.ca/SSG/it03898e.html>> (last accessed: 17 March 2000).

- Power, Michael E. "Digital Signatures and Public Key Encryption Presentation" (1998), online: Treasury Board of Canada Secretariat Chief Information Officer <http://www.cio-dpi.gc.ca/pki/Downloads/Signatures/signatures_e.rtf> (last accessed: 11 March 2000).
- Report to Industry Canada by Domus Software. "Certification and Accreditation for PKIs and Certification Authorities: Survey of Standards, Trends and Identification of Potential Models" (1998) Version 2.1, online: Domus Security <http://www.domus.com/onsecurity/industry_can.pdf> (last accessed: 11 March 2000).
- RSA Laboratories. *RSA Laboratories Frequently Ask Questions* (1996), online: RSA Laboratories <<http://www.rsa.com/rsalabs/>> (date accessed: 11 March 2000).
- Statement by the Press Secretary. "Administration Announces New Approach to Encryption" (September, 1999), online: Center for Democracy and Technology <<http://www.cdt.org/crypto/CESA/whousepress091699.shtml>> (last accessed: 3 April 2000).
- Strick, John C. *The Economics of Government Regulation: Theory and Canadian Practice* (Toronto: Thompson Educational Inc., 1990).
- Szafran, Emmanuel. "Regulatory Issues Raised by Cryptography on the Internet" (1998) 3 Communications Law 38.
- Task Force on Electronic Commerce, Industry Canada. *The Canadian Electronic Commerce Strategy* (1998), online: Industry Canada <<http://www.e-com.ic.gc.ca/english/60.html>> (last accessed: 11 March 2000).
- United Nations Conference on Trade and Development. *Electronic Commerce: Legal Considerations* 1998 UN Doc. UNCTAD/SDTE/BFB/1.
- United Nations Conference on Trade and Development. *Policy Issues Relating to Access to Participation in Electronic Commerce* 1998 UN Doc. TD/B/COM.3/16.
- United Kingdom. "Encryption and Law Enforcement" (1999), online: Cabinet Office <<http://www.cabinet-office.gov.uk/Innovation/1999/encryption/index.htm>> (last accessed: 11 March 2000).
- Wright, Benjamin. "Eggs in Baskets: Distributing the Risks of Electronic Signatures" (1997) XV Journal of Computer & Information Law 18.