UMI

A Bell & Howell Information Company
300 North Zeeb Road, Ann Arbor MI 48106-1346 USA
313/761-4700 800/521-0600

PRIVACY LAW ISSUES FOR ENCRYPTION AND GOVERNMENT CONTROL IN MEXICO

by Mario Ivan Mora Guerra.

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the requirements of the degree of Master of Laws (LL.M.)

The Institute of Comparative Law,

McGill University.

Montreal, Quebec.

November, 1996.

0-612-29837-X

I dedicate this thesis to Amy, my partner in life, who makes my life be beautiful with her smile.

-I.M.G.

ABSTRACT.

Mexico is part of the dramatic change that information technologies are triggering worldwide and is thus subject to the potential risks of privacy that this "digitally conformable" world implies. Encryption may be a solution to this problem, but its use also involves important difficulties that some countries have tried to solve restricting its use, import or export.

This thesis studies the legal challenge of achieving a balanced legislative answer that ensures maximum protection of privacy without conflicting with law enforcement. It also warns the Mexican Consultant Committee on Informatic Policies about the potential problems that the use of encryption technologies will create in Mexico and proposes some solutions.

Mexico is urged to reform its laws pertaining to privacy and confidentiality, and to regulate the illegal and beneficial uses of encryption, in order to achieve a comprehensive and poised legal and administrative infrastructure for information technologies, privacy and encryption. We lay out basic legal parameters to shape a future encryption law in Mexico, emphasizing that the Mexican Government should guarantee that any Mexican can use, develop, market, import or export any encryption product, and that in no event should the Mexican Government impose any compulsory encryption standard. In order to control the criminal use of encryption, we suggest lawful compulsory decryption and certain encryption use restrictions in cases where these technologies are found to have been used to further a crime.

RÉSUMÉ.

Le Mexique fait partie du changement provoqué dans le monde entier par les nouvelles technologies de l'information. Par conséquent la confidentialité des informations concernant ses citoyans est assujetti aux risques que ce monde "electroniquement comfortable" crée. Le chiffrement des donnés peut être une solution pour ce problème, mais son utilisation implique des problèmes quant à la définition de sa régulation que certains pays ont essayé de résoudre en restraignant l'utilisation, l'importation ou l'exportation des programmes de chiffrement.

Cette thése étude le défit légal que répresente la mise en place d'un sytème équilibré qui assurerait le plus grand mesure de confidentialité sans pour autant compliquer l'application de la loi. L'attention du Comitée Mexicain des Politiques de l'information est attirée sur les problèmes que posera l'utilisation des techniques de chiffrement des données au Mexique, et des solutions sont proposées.

Il est suggéré également que le Mexique revoie ses lois en matière de la privacité de l'individu et qu'il régularise les usages positifs et illégaux des programmes de chiffrement. Nous proposons un série des paramètres légaux sur lesquels pourrait se baser une législation en matière de chiffrement au Mexique. De façon à controller l'utilisation criminelle des technologies de chiffrement, nous proposons que le "déchiffrage" des données chifrées soit obligatoire et que l'utilisation des certains méthods de chiffrement se voient restrainte au cas où ses technologies se révèlent avoir été utilisées de façon criminelle. Dans cette législation, il est suggéré que le gouvernement Mexicain garantisse que tout citoyen mexicain ait le droit d'utiliser, de développer, de commercialiser, d'importer ou d'exporter n'importe quel produit ou technique de chiffrement et que le gouvernment n'ait aucun recours à l'imposition d'un modèle standard de chiffrement.

ACKNOWLEDGMENTS

Writing this thesis is the culmination of a great and challenging experience. I am grateful to a number people who directly or indirectly contributed in this process.

First, I want to express my sincere appreciation and special thanks to Professor David L. Johnston for his helpful advises and comments throughout the preparation of this thesis.

I sincerely thank Sunny Handa whose pertinent suggestions helped me put in order my ideas sometimes.

My appreciation to the staff members of the Institute of Comparative Law and to Ann Brodie.

A special vote of thanks to my friend Philippe Prevost, who generously gave his time to help me correcting the final draft of this thesis.

As a CONACYT scholarship holder, I must express my sincere acknowledgment to the National Council of Science and Technology in Mexico (CONACYT), without whose support this thesis would probably have never been written.

Finally, I must mention I am very fortunate in having a specially supportive and encouraging family. My greatest thanks is to my wife, Amy, whose constant and unconditional patience, motivation, and help made this work possible to a great extent. Special thanks to my mother, my sister and my father for their encouraging letters and permanent support.

Table of Acronyms

ARPA	=	Advanced Research Projects Association.
ARPANET	=	Advanced Research Projects Association Network.
CCIP (or the Committee)	=	Mexican Consultant Committee on Informatic's Policies
CONACYT	=	Mexico's National Council of Science and Technology
DES	=	US Data Encryption Standard
EAR	=	US Export Administration Regulations
ECPA	=	US Encrypted Communications Privacy Act
e-mail	=	Electronic mail
EES	=	US Escrow Encryption Standard
FAE	=	Mexico's Federal Act on Fire Arms and Explosives
FAER	=	Mexico's Federal Act on Fire Arms and Explosives Regulations
FAGTI	=	Russian Federal Agency of Government Telecommunications and Information
FBI	=	US Federal Bureau of Investigation
FTP	=	File Transfer Protocol
GSM	=	Global System Mobile
http	=	Hypertext Transfer Protocol
ICC	=	International Chamber of Commerce
IDP	=	Mexico's Informatic Development Program
INEGI	=	Mexico's National Institute of Statistics, Geography and Informatics
IP	=	Internet Protocol

ITAR	=	US International Traffic in Arms Regulations
ITESM	=	Monterrey Technological Institute of Higher Studies
ITESO	=	Western Technological Institute of Higher Studies
KMI	=	Key Management Infrastructure
LAN	=	Local Area Networks
LEAF	=	US Escrow Encryption Standard's Law Enforcement Access Field
Meeting	=	Organization for Economic Cooperation and Development's (OECD's) Meeting of Experts on Cryptography
MEXNET	=	Mexican Network
MILNET	=	Military Network
NDP	=	Mexico's National Development Plan 1995-2000
NIST	=	US National Institute of Standards and Technology
NSA	=	US National Security Agency
NSF	=	US National Science Foundation
NSFNET	=	US National Science Foundation Network
OECD	=	Organization for Economic Cooperation and Development
PGP	=	Pretty Good Privacy
Pro-CODE	=	Promotion of Commerce Online in the Digital Era Bill
RF	=	Russian Federation
RSA	=	Rivest-Shamir-Adelman public key crypto-system
SAFE	=	Security And Freedom through Encryption Act

SCSSI	=	France's Prime Minister Services Office
SEP	=	Mexican Ministry of Education
TTP	=	Trusted Third Parties or Certification Authorities
UdeG	=	University of Guadalajara
UDLA	=	University of Las Americas
UNAM	=	National Autonomus University of Mexico
URL	=	Uniform Resource Locator
WAN	=	Wide Area Networks
WWW	=	World Wide Web

PRIVACY LAW ISSUES FOR ENCRYPTION AND GOVERNMENT CONTROL IN MEXICO

TABLE OF CONTENTS

page

Preface.

A Technological Revolution.

Just like the industrial revolution brought about an expansion of the physical capacities of the human being, today information technologies are expanding human beings' intellectual capacities. Improvements in information technologies have a critical impact in the global context today, transforming production structures, trade in goods and services, communication services, research facilities and job opportunities. Mexico is no exception to this experience. Our daily lives have a continuous connection with these technologies because they can be easily incorporated into almost every aspect of human activity.

The Information Highway.[1]

"It is clear that information technologies are modifying -and will modify even more- our daily lives, our impression of the world, and the way we interact with it. These examples, among others, evidence the importance of information technologies as a strategic tool for the development of countries in the rest of this century and, of course, in the forthcoming century."[2]

[1] The term information highway refers to "existing public and private networks. They include satellite television, digital and traditional airwave radio, broad band, narrow band and wireless (e.g. cellular telephone, plus local area (LANs) and wide area (WANs) computer networks and databases. See: D. L. Johnston, D. Johnston & S. Handa. *Getting Canada On Line: Understanding the Information Highway.* (Toronto: Stoddart Publishing, 1995) at 4. "The Information Highway is a manifestation of a deep and broad technological change in all segments of our society". *See:* Minister of Supply and Services. *Connection Community Content. The Challenge of the information Highway.* (Canada: Final Report of the Information Highway Advisory Council, September 1995.)

[2] *See: Meeting to introduce the Informatic Development Program 1995-2000,*

Mexico Online.

Mexico is immersed in globalization. Since the country's entry to the General Agreement of Tariffs and Trade -now the World Trade Organization (WTO)- within the last decade, it has taken important steps towards an open economy. In order to continue this journey, a number of things must be accomplished, in particular, the connection of Mexico to the Information Highway. The aptness with which Mexicans incorporate the information highway into their daily reality will be critical for the realization of a number of objectives, such as the industrial competitiveness of the nation, and a higher level of Mexicans' well-being.

It is a fact: information technology affects our lives today in many different senses and its advances are giving new shape to the countries' economies, as the communication technologies come together in a single "highway" that can be easily accessed almost by everybody.[3] This open access, however, gives rise to a number of interesting questions.[4] In this thesis, we focus on information security issues to protect privacy[5] online.

April 12, 1996. Presentation speech by Dr. C. M. Jarque, Chairman of the National Institute of Statistics, Geography and Informatics (Mexico City, National Institute of Statistics, Geography and Informatics) at 3, available online at Uniform Resource Locator [hereinafter URL] http://inegi.gob.mx/homepara/pdi/.

[3] *See:* Minister of Supply and Services, *supra*, note 1, at vii.

[4] For instance, there are lots of literary works already published -and products offered- online. We wonder what the parameters are going to be to control copyright on the digital revolution. What answers are going to emerge as to the control of obscenity published over global communication networks? Whose law applies on the online world? How are contracts formed on cyberspace?

[5] Privacy is defined "in two ways: the right to be left alone, and the right to exercise control over one's personal information... Personal data protection has been defined as the claim of individuals to determine when, how and to what extent information about them is communicated to others. Data protection is an aspect of privacy protection that involves control over the collection, storage, accuracy, use and dissemination of personal information." *See:* Minister of Supply and Services. *Privacy and the Canadian Information Highway: Building Canada's Information and Communications Infrastructure.* (Canada: Industry Canada, October 1994.), at 5.

Communications that travel through the information highway can be intercepted and altered before they reach their destination. If the communication is intercepted, then it is not private anymore, and if the data or the sender's information it contains is altered, the communication will not be authentic when it reaches its destination. So, how can the parties of a digital communication assure the confidentiality and authenticity of their messages in this risky environment?

Mexico lacks a legal framework that assures privacy and confidentiality on electronic communications or protection on data storage. In this study, we raise legal questions, answers and rationale on certain privacy law issues for encryption[6] in Mexico, analyzing this country's entry onto the Information Highway. We limit the scope to security and privacy topics; we exclude contract and criminal law and the economic or social impact of Mexico's connection to the online world.

The Role of Encryption in the online world.

Advances in encryption technologies are increasingly ensuring personal privacy and security. Today it is harder, and sometimes impossible, for governments to intervene[7] on telephone lines, intercept and read electronic mail [hereinafter e-mail] messages and other kinds of protected information electronically stored or sent.

Incredible amounts of data run worldwide electronically. However, this course is risky: before the information reaches its

[6] Encryption is the art of encoding information, so only the person to whom it is addressed can read it, but it also represents "an indication of user's distrust of the security system, the owner or the operator of the system, or law enforcement authorities." Rose, Lance. *Netlaw: Your Rights in the Online World..* at 182.

[7] The term "wiretap" is often used to describe the interception of others' telephone lines. The term, however, seems to refer to "wire" phone transmissions. In this study, we will not use the term in this latter sense, but refer to both wire and wireless communications.

destination, it normally crosses several potential interception points.

Encryption has a critical role to play, not only in the data security development context, but also in the global economic context, ensuring personal, commercial or government data transmission. Almost any large enterprise can be the target of industrial espionage; many people -under investigation or not- can be subject to "wiretapping" without knowing it; and Government information also represents a very important target for hackers.[8]

Although commercial and contractual issues are not part of this work, the security measures taken to electronically transmit documents and exchange messages will have important consequences in these fields. Why? Electronic commerce faces three main legal difficulties: the "paperless" way of doing transactions, the absence of physical or geographical boundaries in the *online* environment, and the security measures that people will have to take, and rely on, to engage in these transactions.[9]

A Global Challenge for Law.

On the global scale, the challenge for the current law to respond to new conditions in communication media is a great one. Traditional paper means of keeping and transmitting information will

[8] This term applies to people who break into private files without permission, steal computer passwords or inflict computer viruses intentionally into other people's computers or networks. Another term is "crackers". "Crackers are able to attack targets halfway around the world with no fear of prosecution... Everywhere you look, bright, clever people are breaking into communication systems, industrial control systems, transportation systems, health care systems -- anything and everything that's controlled by networked computers." *RSA's Data Security Conference*, Remarks prepared by R. Ozzie, available online at URL http://www.lotus.com/notesr4/ozzie.htm. January, 1996, at 1. The author of these remarks stresses that computer progamme cracking is "a direct result of our having moved into the information age without adequately securing our information and our global information systems" at 1-2.

[9] For a very comprehensive discussion of legal-commercial implications of online transactions in the U.S., *see*: T. J. Smedinghoff, Ed. *Online Law: The SPA's Legal Guide to Doing Business on the Internet*. (Massachusetts: Addison-Wesley, 1996) at 4.

be almost completely removed. Furthermore, the geographical borders within which laws operate today will be almost erased.[10]

Even though law must not be static, but dynamic and able to adjust to new technological developments, its response to these new technologies is often very slow and vague; Mexican law is no exception to this fact. The reason is that technology changes so rapidly that there is almost no time to consider it thoroughly. To deal with this situation is an extraordinary challenge for law worldwide.

Mexico's Legal Answer to the Information Age.

Legislative answers to new information technologies have yet to be given. This legal field is almost completely barren, and the problems related to it will increase. What legislation should Mexico enact? What issues may arise? What legal response is appropriate? Does Mexican legislation provide a satisfactory level of protection for privacy online? What parameters regulate encryption technologies in Mexico? How will Mexican courts face cases where evidence is encrypted? We focus on encryption as the answer for most of today's security needs. One of the core points of this study is the balance that must exist in any encryption legislation between law enforcement concerns and privacy protection. The debate that has emerged thereon in the USA will also be examined.

Thesis outline.

This study proposes legal reforms to the Mexican Consultant Committee on Informatic Policies for revision to Information Technology Law in Mexico, as they relate to information security measures and encryption.

[10] For instance, an electronic-mail message can cross several states and countries before it reaches its destination.

In Chapter One, we describe the electronic information flow with special emphasis on the Internet and its history, particularly in Mexico. Then we consider the security measures concerning electronic information flow. Private and public key cryptosystems are examined as possibilities for ensuring electronic privacy and security, with special attention to "Pretty Good Privacy", one of the most important cryptosystems today. Then we discuss digital signature technology as the means to confirm the identity of the subjects on electronic communications, and ensure the authenticity of their message exchange.

Chapter Two is devoted to the study of legal treatment of encryption in other countries. The comparative technological basis is the USA because of the obvious impact that American technologies have worldwide. The legal bases are the French, Russian and Japanese encryption laws. They represent some of the most important efforts, even though there are strong differences among them, to legislate for encryption in the world today.

An important concern of this study is the balance between law enforcement preoccupations and privacy protection concerns that any encryption law should achieve. In this respect, the US law is particularly helpful, since it represents the environment where a large-scale debate has taken place on the subject, producing positive results. We analyze the US Data Encryption Standard and the Escrow Encryption Standard, as examples of governmental efforts to establish encryption standards. We also describe the US export controls on encryption and their relative effectiveness in controlling spread of strong encryption technologies worldwide. We then examine the leading cases on encryption and their legal implications on US law, emphasizing ideas that may help to shape encryption laws in Mexico.

Chapter two ends with a study of the Organization for Economic Cooperation and Development's [hereinafter OECD]'s Meeting of experts on cryptography. We analyze its interest in escrow systems, stressing its implications for a potential global encryption regulation.

Chapter Three, deals with privacy issues in Mexican Law. We study the Mexican Government's actions to get Mexico online, focusing on the National Development Plan's [hereinafter NDP]'s creation of the Informatic Development Program and the Consultant Committee on Informatic[11] Policies. We analyze the initial proposals of the Program and make some important recommendations.

We then study Mexican legislation applicable to security and privacy on Information Technologies, and identify some important deficiencies related to legislation and the Mexican Government's actions. Using the OECD's Meeting's conclusions, we consider some constitutional implications of a hypothetical escrow system in Mexico.

In Chapter Four we make recommendations to the Mexican Consultant Committee on Informatic Policies for revising security and privacy law in Information Technology.

Thesis purpose.

The main purpose of this study is to advise the Mexican Consultant Committee on Informatic Policies on a balanced answer to the debate between personal privacy and crime control. The answer must ensure maximum personal and commercial privacy without undermining the State's need for protection and law

[11] *See*: *Infra*, note 184 for a description of this term.

enforcement.

We urge Mexico to adjust its laws to new technological developments, to regulate privacy and confidentiality, and to define the illegal and the beneficial uses of encryption.

We propose that every Mexican should have lawful access to use any encryption program. We suggest that the Mexican Government refuse to impose any compulsory encryption standard or system that requires the delivery of a copy of the citizen's private decryption keys into the Government's hands.

We hope to start the Mexican discussion on important encryption topics and show how the Government can legislate an encryption system that protects personal and commercial privacy, ensures effective law enforcement, imposes limitations on the State's authority and, thus, preserves Constitutional guarantees.

CHAPTER I. GENERAL CONCEPTS

1. Communication by networks.

2. What is the Internet?

- Some important concepts in connection with the Internet.

A) History of the Internet. Some reasons for its growth.

B) Internet and Mexico.

3. Security measures in the electronic transmission of documents.

A) Data encryption.

i) Symmetric or private key cryptography.

ii) Asymmetric or public key cryptography.

B) The "Pretty Good Privacy" encryption system.

C) Message authentication and digital signatures. The confirmation of the identity of the subjects.

- Some legal aspects about Trusted Third Parties.

CHAPTER I. GENERAL CONCEPTS.

The information highway[12] is a term which is often referred to in this study. It has been defined in several senses,[13] almost all of which mention the following characteristics: first, the information highway has caused a transformative revolution; second, it spreads all around the globe; third, it encompasses many technological innovations that affect our every-day life; and fourth, it is a "network of networks" transmitting and transforming data, audio and video.

The term is not completely precise, though, because it excludes a number of important issues that are embodied into its real meaning and extent. Consequently, sometimes it is misconstrued, and only refers to a simpie source of information.[14] Hence, when we further refer to this term, we will not only mean a simple source of information, but the means through which large numbers of communities may communicate with each other in a very effective way.

Human communication is mostly what the information highway

[12] *See* definition *supra* note 1.

[13] Its origin is to be found back in 1992. US Vice-President Al Gore made the term popular in the 1992 Presidential Campaign: one of the reasons to describe the phenomenon with the word "highway" is the metaphor of a carriage way through which can flow an impressive volume of data. For further reference on the topic *see:* D. L. Johnston, D. Johnston & S. Handa. *Supra* note 1 at 5 through 7.

[14] *See ibid.*, for instance, stating that the term information highway "ignores the essential element of people and communities maintaining contact with one another" (at 5). The authors propose the more comprehensive term "global village square", which includes the features of uniting people for many different purposes.

is about. Privacy and secrecy[15] are two very important parts not only of human communication, but also of human life, because they are closely connected to individuals' autonomy. The ability to keep secrets and selectively disclose some of them allows people to distinguish themselves from others. Sometimes secrecy and privacy are as critical as communication is for human life itself.

One of our concerns is precisely the way in which we can preserve our privacy even within the broad boundaries of the information highway.

1. Communication by networks

An electronic communication is the data transmission -in any of its forms: images, sounds, writing characters, signals or signs- by wire, optic fibers, cable, radio, micro-waves, satellites, electromagnetic or photoelectric systems.[16] An information system is a method to generate, send, receive, store or otherwise process data messages.[17] The communication network connects different information systems to allow the transfer of information between places physically separated.

[15] Privacy is "the condition of being protected from unwanted access by others-either physical access, personal information, or attention". M. A. Froomkin, *"The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution"*. 143 U. Pa. L. Rev. n3, 712. "'Secrecy' refers to the intentional concealment of information so as to prevent others from 'possessing it, making use of it or revealing it' to third parties... [and] it also refers to 'the methods used to conceal [information], such as codes or disguises'". *Id.* at 712.

[16] Article 3-XIV of the Federal Telecommunications Act. Published in the Federal Register (*Diario Oficial de la Federación*) on June 7th., 1995. Mexico.

[17] *See*: M. A. Froomkin. *Supra*, note 15 at 789, quoting 18 U.S.C. s. 2510(12). For further reference *see also:* Minister of Supply and Services. *Supra*, note 1 at 3-4.

2. What is the Internet?

The Internet is a global link of thousands of computer networks, which are owned by different people. It connects government-operated networks, commercial networks, business networks, research networks and other smaller independent networks.[18]

The Internet represents one of the most important examples of technology convergence today.[19] It links an enormous number of computer databases that are spread all around the world, through satellites, microwaves and a series of telephone lines dedicated to telecommunications.

Some important concepts in connection with the Internet.

Today's "links" of the Internet are available in a variety of degrees: it comprises high-capacity telephone lines, fiber optic links, satellites, microwaves, lasers, etc. This structure is recognized as the Internet's "backbone".[20]

[18] The Internet is not owned by one single person or group, and there is not a comprehensive body of law that exclusively applies to it. *See:* R. P. Klau & J. Heels, *"There is still not a single comprehensive resource for learning about the law that relates to the Internet."* Student Lawyer. November 1995, at 12.

[19] The term "convergence" means, for information technology purposes, "the merger of communications and computer technology based on a common digital language". *See* D. L. Johnston, D. Johnston & S. Handa. *Supra,* note 1 at 7.

[20] *Cfr.* Barrister, Ed. *"Who Has the Right of Way? Intellectual Property Rights on the Internet."* (1996) 22, Barrister Magazine. No. 4, at 25.

There is a wide range of options to access the Internet. The main methods are: Electronic mail, Telnet, File Transfer Protocol [hereinafter FTP], Netscape, and, of grater importance today, the World Wide Web [hereinafter WWW]. We will briefly describe some of these sources:

A *Network* is the connection of two or more computers that communicate to each other. This is why everybody says that the Internet is a "network of networks."

E-mail allows the exchange of messages between two connected computers. This connection can now be made by local or commercial networks through a modem (*i.e.*, the apparatus that connects a computer with a telephone line, converting digital information into sound signals and vice versa.)

Telnet is a program that connects users to Internet hosts; the user can then use the programs available in that host as he was locally connected to it.

The *FTP* is the oldest of the file transfer methods used on the Internet; it allows its users to download public files and transfer files from one computer to another.

Netscape is a frequently-used program that allows its users to "explore" the Internet, through its millions of servers, and get multi-media information.

The *World Wide Web* [21] [hereinafter WWW] is one of the most important multi-media based information sources; it has become an essential part of the Internet. It allows users to navigate on a "point and click" basis, through different Web browsers. The sites' format include text, "hypertext" (*i.e.* text that is linked to another related site or document), sound, color graphics and video images.[22]

[21] *See also* the term "World-Wide Web" in *The Free On-Line Dictionary of Computing*, available online at: URL http://wombat.doc.ic.ac.uk/?World-Wide+Web.

[22] *See*: Barrister, Ed. *Supra*, note 20 at 25.

A) History of the Internet.[23] Some reasons for its growth.

The Cold War brought the United States and the Soviet Union close to a nuclear encounter in the 1960's, with the US fearing an attack from the Soviets. The US Defense Department had to take action, and it did. As a result it emerged what would become the first stage of the Internet.[24]

The origins of the Internet are to be found in 1969 when the US Defense Department contracted, through Advanced Research Projects Association [hereinafter ARPA], the firm Bolt, Beranek and Newman to design and develop a computer net to connect the Stanford Institute of Investigation, Utah University, the University of California in Los Angeles and the University of California in Santa Barbara.

The objective was to ensure that communications between two separate locations, in this case the Pentagon and the scientists working on defense projects, would not be interrupted in case of nuclear emergency. This required the creation of a network that would be able to alternate the flow of information by different channels if one link failed. This goal was achieved by the 1970's with the creation of the ARPA network -or ARPANET. The net grew with time, permitting information flow between universities' researchers

[23] For a very comprehensive study on the history of the Internet, *see*: V. Cerf, *"A Brief History of the Internet and Related Networks"*, available online at: URL gopher://gopher.isoc.org:70/00/Internet/history/_A Brief History of the Internet and Related Networks_ by V. Cerf. *See also:* B. Aboba. *"How the Internet Came to Be"*, in *"The Online User's Encyclopedia"* (1993), available online URL gopher://gopher.isoc.org:70/00/Internet/ history/how.internet.came.to.be.

[24] *See generally*: D. L. Johnston, D. Johnston & S. Handa. *Supra*, note 1 at 16 through 19.

and other Institutions thanks to the Internet Protocol [hereinafter IP].[25]

Between the 1970's and the 1980's, ARPANET expanded its "nodes" from 50 or so, to 200, allowing its users not only to exchange investigation data, but also to use private e-mail boxes to exchange other kinds of information, even personal.

Around 1980, these work stations, which in the beginning were shared by a large number of users, were transformed into a number of personal computers. During the 1980's decade, ARPANET became the international standard, and Local Area Networks [hereinafter LAN]s began running over telephone systems.

By 1983, ARPANET was divided into two parts: the Military Net [hereinafter MILNET] and a smaller public Net. The term "Internet" was then used to describe the sum of the two systems.

The IP was designed to ease the data flow between a large number of networks, allowing computers to communicate despite technical differences, although at that time there existed only the two networks we have just mentioned.

In 1984, the National Science Foundation created NSFNET,[26] a net made of several regional nets, which provided five super-computer centers to permit access to any educational Institution.

The Internet has reached huge dimensions today (November 1996), allowing 146 countries to communicate through its 636,000 educational and 550,000 commercial networks. It counts around 50,000,000 users worldwide.[27] The numbers are never exact because of the exponential growth of the Internet.[28]

[25] *See generally*: V. Cerf, *supra*, note 23.

[26] *Ibid.*

[27] *See* URL http://www.commerce. net for an estimate of users updated frequently. *See also* URL http://home.netscape.home/newsref/pr/newsrelease69. html.

[28] *See*: *Infra*, graph 1 "Internet evolution", at 152.

Most of the reasons for the Internet's growth converge on several points: economic global coverage, speed, and ease to get and transmit any kind of information. The system links people looking for goods, services, professionals and expert fora, clients or potential clients, conversation groups in practically all fields and levels, etc.

B) Internet in Mexico.

Mexico has a very recent Internet history.

It all began in 1989 with the connection of the Monterrey Technological Institute of Higher Studies [hereinafter ITESM] to the University of Texas in San Antonio. The National Autonomus University of Mexico [hereinafter UNAM]'s Network began in 1990, with the service provided by BITNET, which functioned through NSFNET. Then, other Universities were connected: the University of Las Americas [hereinafter UDLA], the Western Technological Institute of Higher Studies [hereinafter ITESO] and the University of Guadalajara [hereinafter UdeG], forming what became RedMEX [hereinafter MEXNET, as is called today]. Later, the National Council of Science and Technology [hereinafter CONACYT] and the Ministry of Education [hereinafter SEP] became part of MEXNET. E-mail, discussion lists and FTP were the first facilities added to MEXNET.

In 1992, MEXNET incorporated the "Gopher" search system, and it was not until 1993 that the most important data bases and the first electronic magazines were elaborated.

By 1994, the UNAM's Network offered new services, such as journals, entire book texts, search by word (using the "Veronica" server). MEXNET and CONACYT together formed the National

Technological Net [hereinafter RTN] in that year, and by 1995 there were a large amount of services available on the RTN by virtue of the connection with the WWW, such as video conference. In December 1995 the Internet was commercially available through the Nets Information Center of Mexico [hereinafter NIC-Mexico], which currently coordinates the growth and expansion of the Internet in the country.

Today, there are many Internet Service providers in Mexico; commercial "domains" (or addresses) have grown impressively.[29]

3. Security measures in the electronic transmission of documents.

Information security is a core legal issue involved in electronic communications. It raises questions about the authenticity and integrity of the messages, as well as about the confidentiality or privacy of their contents. Certain messages, for instance those involving sensitive contract negotiations, a company's trade secret information, or credit card information sent through the Internet, require a high degree of privacy.

One of the basic requirements of the Communication Infrastructure is security because it must provide an appropriate environment for the privacy and confidentiality of the messages involved. Electronic communications infrastructure should then ensure the authenticity and integrity of the message to the parties. It

[29] In general, de demand of informatic products in Mexico has grown enormously since 1989. *See*: *Infra*, graph 5, "Informatic market in Mexico", at 156.

is also convenient that communications be "signed" by the parties, and that, for instance, the parties can have some secure electronic payment options as well.

When talking about privacy and security, we must bear in mind that privacy refers to the confidentiality of the information, and that security means integrity of the message in order to assure that it has not been altered during its transmission.

In this electronic age, everybody must take whatever security measures are available for protecting his/her own work and data. "Traditionally, we accomplish this through physical security measures... This was fine when we used only paper documents,"[30] but is no longer enough, since today almost all important information is electronic and stored on computers.

"Threats to the confidentiality of a message come from two primary sources. The first is from those who provide the communication networks through which the message travels... The second threat comes from third parties who obtain access to the network (lawfully or otherwise) and intercept, read and disclose the contents of a message." [31]

Whenever a computer or a computer disk is stolen, or its content intercepted, the information it contains can be, however, assured with encryption. Some measures of physical security, are, nevertheless, necessary. For example, private network's file servers must be located in places with high-security doors, and must contemplate some network security measures. Unauthorized access is frequently avoided by the use of a login for each user. Each user has a secret password that enables him or her to access his/her personal files in the network. There are also some programs that provide for power-on password protection. Network file servers can use an encrypted password to prohibit intruders accessing the

[30] J. L. Kashi, *"Protecting Client Confidences in the Electronic Age."* [1995] Law Practice Management, at 22.

[31] See: T. J. Smedinghoff. *Supra* note 9, at 11-12.

password list. Really sensitive commercial or corporate data should be kept encrypted too.[32]

Viruses represent another important risk that can be controlled by using some frequently-updated anti virus programs. Another problem is that erased materials can remain somewhere around the disk and can be, thus, recovered by almost anybody. This is often handy, in case of accidental erasing of data, but can represent a problem. If erasing of data is intentional (for any cause) and some trespasser has the possibility of recovering those data, it can be harmful to the data owner. Some programs provide a solution for this by a command named "purge" that definitely erases any "deleted" files.[33]

Security over public networks (such as the Internet) is even more complicated, and some even advise, for the moment, not to have any computers that keep important or sensitive data connected to the Internet,[34] or to connect these computers through a modem and a dial-up provider only for the time of use on the Internet.

A) Data encryption.

Cryptography[35] is the use of methods to disguise messages. This can be achieved by using, for instance, codes and ciphers. The *code* is a communication system that relies on a pre-arranged set of meanings. A *cipher* is the mathematical function for encrypting and

[32] *See*: J. L. Kashi. *Supra*, note 30 at 22-23.

[33] *Ibid.*

[34] *Ibid.* at 26.

[35] There are many important crossing points between law and encryption. This study, however, does not deal with intellectual property encryption issues.

decrypting messages; ciphers are also called *algorithms*.[36]

To encrypt a message is to transform its data into an unreadable form for anyone who doesn't have a determined code or secret *decryption* key. The purpose of this process is to ensure privacy by keeping the information out of the reach of any intruder or any one to whom the information is not addressed. In general, data encryption is made by *encyphering* the message. The message is scrambled up, in a very complicated way, so that only the person who owns the key can open it up.

Encryption allows secure communications over insecure channels, even in multi-user settings. The general picture of this consists of one person (the sender) who wants to transmit a message to another (the receiver) so that only that person and no one else can read it. The message (which is also called *plaintext*) is encrypted with an encryption key and is now called *cyphertext*. Once the receiver wants to open the message, he/she will have to use the decryption key. Only then can the plaintext be recovered from the cyphertext.

Strong cryptographic methods, *i.e.* cryptographic products that use a key bigger than 56 bits,[37] were subject to certain restrictions and, thus, only used by Governments (to keep state secrets, military and diplomatic information, etc.) and by the finance sector (to protect electronic transactions, electronic fund transfers, etc.) Today, stronger cryptography[38] is available for individuals, so

[36] *See*: Committee to Study National Cryptography Policy. (Computer Science and Telecommunications Board; National Research Council; National Academy of Sciences and National Academy of Engineering.) May 30, 1996. *Cryptography's Role in Securing the Information Society. Overview and Recommendations.* Available online at: URL http://www.lotus.com/notesr4/crypt-or.htm. *See also:* T. J. Smedinghoff. *Supra* note 9, at 12.

[37] A bit is the smallest piece of information, that consists either in a number zero or one. Eight bits form a byte, which then forms a character. 56 bits represent a 7-character key.

[38] For example the Pretty Good Privacy system, which is considered a military-level method, and uses a key bigger than 128 bits. *See*: P. R. Zimmermann. *The official PGP User's Guide.* (Cambridge, Massachusetts: MIT Press. 1995). Available online URL fttp://net-dist.mit.edu/pub/PGP/

everybody can enjoy high protection on their own personal and commercial affairs.

Cryptography has two main variations: *symmetric* cryptography, in which a single private key is used to encrypt and decrypt the message; and *asymmetric* cryptography, in which there are two keys: the public one and the private (or secret) one. Symmetric cryptography implies that the sender and the receiver will have to agree, by secure means, on a single private key to exchange messages. The second means two things: first, that each person will have his/her own "pair" of keys, a public key and a private key, the public key being known by everybody. Second, data encoded with either of the two keys can only be decoded with the other.

Cryptanalysis is the procedure for breaking the codes and ciphers in order to decode certain cyphertexts. *Key escrow* is the practice of duplicating the key to a cipher, so that a third party can decrypt messages using that cipher.[39]

Strong encryption methods can protect electronic records and communications in such a way that they can impede disclosure and interception even from sophisticated Government agencies, such as the National Security Agency [hereinafter NSA] in the USA.

Cryptographic products can contribute in an important number of ways to commercial, personal, and Governmental ends.[40] Among users of cryptography, we can distinguish: banks;[41]

[39] "As used in the Clipper Chip debates, the term 'escrow' is something of a misnomer because the escrow is primarily for the benefit of the Government rather than the owner of the key." *See*: M. A. Froomkin. *Supra*, note 15 at 715.

[40] National Security-related and Diplomatic secrets, for instance, are kept and communicated under strong cryptographic methods. *See* article 52 of the Mexican Foreign Service Act's Rules (*Reglamento de la Ley del Servicio Exterior Mexicano*). published in the Federal Register(*Diario Oficial de la Federación*) on October 11th., 1994. *See also*: L. J. Hoffmann *et al.* *"Cryptographic Policy"*, (Comm. ACM, Sept. 1994), at 109-111, noting that an average of $1 trillion passes daily by the Clearing House Inter bank payment system, via wire and satellite.

[41] Banks in the US are required by the Department of the Treasury to encrypt all electronic funds transfer messages. *See*: G. Murphy, *US Department of the Treasury, Directive: Electronic Funds and Securities Transfer Policy-Message Authentication and Enhanced Security*, No. 16-02 s. 03 (Dec. 21, 1992). *See also*

automated teller machine [hereinafter ATM]'s users; electronic transactors; businesses with commercial and trade secrets; all kinds of professionals; users of telephones, e-mail,[42] fax or computers; and also criminals.[43]

i) Symmetric or private key cryptography

Traditional cryptography (also called private-key or secret-key and symmetrical cryptography) is based on the presumption that the sender and receiver of a message know and use the same secret key, both to encrypt and to decrypt the message. The main problem for the sender and receiver is to confidentially agree on the private key to avoid later unauthorized reading of encrypted messages, in case anyone else finds out or intercepts the secret key.[44]

The generation, transmission and storage of keys (also called "key management") is an issue that all cryptosystems must deal with. However, secret-key cryptography may have some difficulty providing secure key management. Why? In private key cryptography, whenever the parties are in two separate physical locations and want to transmit the private key, they have to share some private information. Key transmission, thus, will have to take place through

generally: Schneier, Bruce. *Applied cryptography* (US: John Wiley & Sons, 1994).

[42] Electronic mail messages transmitted through public systems -such as the Internet- can be intercepted, unfortunately, with ease. *See*: R. Abramson, *"Protecting Privilege in E-mail systems"*, (1994) Legal Times, at 29. *See also generally*: Kashi, J. L. *Supra*, note 30.

[43] One important cause for this is that cryptography not only allows people to keep information in secret, but also to keep *identities* in secret. For a larger description of all the above-mentioned different uses *see*: M. A. Froomkin. *Supra*, note 15, at 718-735.

[44] *See*: P. Fahn. *"Frequently Asked Questions About Today's Cryptography"*, (May 5th., 1995), available online at: URL ftp://pub/usenet/news.answers/ cryptography-faq/RSA/

an alternative and "secure" communication channel that will normally consist of some conventional message transmission system, such as a courier service or a telephone communication. The question here is: if there exists an alternative secure channel for the parties to agree on the secret key, then why using encryption to have privacy in further message flow and not using this other secure channel?

This system, however, is used by the US Federal Data Encryption Standard [hereinafter DES], which we examine later.[45]

ii) Asymmetric or public key cryptography

Public-key cryptography was invented by Whitfield Diffie and Martin Hellman in 1976 with the intention of making easy the “secure” key transmission problem.[46] Everybody's public keys are published to enable encrypted communications, while private keys are kept in secret. Communications only involve public keys, and no private key needs ever be transmitted or shared. Public-key cryptography can also be used for authentication (digital signatures) as well as for privacy (encryption).

Asymmetrical cryptology, or public key cryptology, uses a system different from the private key's system. It consists of a set of two different keys for every individual: a public one and a secret (or private) one. Only the public key of that specific set can "pair" and decrypt messages encrypted using the private key of this set, and vice versa. The public key is known to everybody. Thus, a confidential message from "X" to "Y" will have to be encrypted by "X"

[45] *See: Infra*, Chapter II, part 1.

[46] *See*: P. Fahn. *Supra*, note 44.

using "Y's" publicly known key. Once this message reaches "Y", only he/she will be able to read it, decrypting it using his/her own private key. When "Y" responds to "X", the answer will be encrypted by "Y" using "X's" public key, so only "X" can open it up using his/her private key.

It is obvious that one important requirement is that the private key is not connected to the corresponding public key, so that the former cannot be inferred from the latter.

A major advantage of public-key cryptography over private key cryptography is the increased security, since no private key needs ever be transmitted or revealed to anyone. By contrast, in a secret-key system there is always a chance for an intruder to discover the single secret key while it is being transmitted, and thus to gain further access to the once confidential message flow.[47]

Another important advantage of public-key systems over private key ones, is that the former can provide digital signatures as an authentication method, and not the latter. In private key systems, this method requires trust in a third party, which keeps a central database with copies of all users' secret keys.[48] This can be a serious problem because it could mean repudiation of the message (even if it was already signed by the sender) in case one of the parties sharing the secret key somehow has compromised or revealed it, or in case of an attack on the database. In other words, digitally signed messages can be proved authentic to a third party, such as a judge, allowing such messages to be legally binding. By contrast, it would be difficult for a message to be legally binding if it was transmitted under insecure circumstances, as in the cases described above. The public-key authentication system avoids this type of repudiation since each user has the sole responsibility of protecting his/her private key. This feature is called "non-

[47] *Cfr.* T. J. Smedinghoff. *Supra,* note 9 at 499-501.

[48] *Ibid.* at 47-49, describing the certification process, and the certification authorities' functions.

repudiation".[49]

Public-key cryptography is not intended to replace secret-key cryptography, but rather to supplement it and make it more secure. In fact, the first use of public-key systems, which is still one of its primary functions, was the secure exchange of keys over secret-key systems.

Public-key systems are an important part of this study: they represent the best choice for protecting personal privacy. At the same this feature makes it harder for Governments to interfere or disclose encrypted data (stored or transmitted). Consequently, an important debate arises here.[50]

B) The Pretty Good Privacy encryption system.

Among the available security softwares, "Pretty Good Privacy"[51] [hereinafter PGP] is one of the most popular. PGP is an asymmetric cryptography system that ensures elements such as privacy and authentication. This means two important things for the purposes of information security. First, the privacy of the message is guaranteed, so that only the person to whom the message is addressed can read it. Second, message authentication is ensured, giving certainty as to the origin of the message.

PGP is an asymmetric type of cryptography which implies it does not need alternative secure channels to transmit or exchange

[49] *Ibid.* at 55 for further reference on non-repudiation.

[50] *See infra*, Chapter II, part 3, when we outline this debate. *See also:* US encryption cases of Zimmermann, Karn and Bernstein, *infra*, Chapter II, part 3, section C), subsections i) through iii).

[51] *See*: P. R. Zimmermann, Philip R. *Supra, note* 38.

keys. This is a definite advantage. Moreover, the user is the only one to know and choose his/her own private key.

PGP uses the Rivest-Shamir-Adelman [hereinafter RSA][52] public key crypto-system,[53] and combines it with the digital signature feature.

Digital signatures allow PGP to offer message authentication. This means that the person who receives the message can be sure that the message was effectively originated by the person who appears as the sender. The way to confirm this is by including the digital signature of the sender in the message: the message is first encrypted with the sender's private key, and the receiver's public key. The receiver will open the message using his/her private key and the sender's public key to decrypt the message.

C) Message authentication and digital signatures. The confirmation of the identity of the subjects.

Among the available information security measures, digital signatures seem to be the most promising in satisfying important communications requirements, such as authentication and non repudiation of the messages.

[52] For further reference about RSA, *see: "Current controversy surrounding RSA"*. Available online at URL: http://www.library.carlton.edu/student-workers/dan/rsa.htmL

[53] RSA is a public-key cryptographic system that works for both encryption and authentication. It was invented in 1977 by Ron Rivest, Adi Shamir, and Leonard Adelman. *See*: P. Fahn. *Supra*, note 44, stating that RSA "...works as follows: take two large primes, p and q, and find their product n = pq; n is called the modulus. Choose a number, e, less than n and relatively prime to (p-1)(q-1), and find its inverse, d, mod (p-1)(q-1), which means that ed = 1 mod (p-1)(q-1); e and d are called the public and private exponents, respectively. The public key is the pair (n,e); the private key is d. The factors p and q must be kept secret, or destroyed."

Digital signatures are intended to be the electronic replacement of hand-written signatures. Digital signatures, however, are not digitized versions of the sender's manual signature.[54] Like handwritten signatures in printed documents, digital signatures work to assert that the person whose signature appears on the document actually wrote it, or at least agrees to it. The receiver can then verify both, that the document originated from that named person, and that the content of the document has not been altered, as will be shown later on. The first of these two characteristics is called "authenticity of the sender"; the second is the "integrity" of the message. Their purposes are the same: to identify the sender of a certain message and to ensure that, once the message has been received, the sender can not deny his/her sending it. This is known as authentication in the digital context.

As mentioned above, digital signatures can also guarantee the integrity of the message, because each signature is different for each message. Yet, if a particular message is disclosed by someone who it is not the intended receiver, the message digest and the message itself will not be equal. This means that either the message originated elsewhere or was altered after it was digitally signed.

The procedure for signing a message is mainly as follows:[55] in order for the sender to digitally sign a message, he/she runs a computer program that includes the feature of the digital signature. The program "creates a message digest (or hash value) of that communication. Then it encrypts the resulting message digest using the sender's private key. The encrypted message digest is the digital

[54] *See*: T. J. Smedinghoff. *Supra*, note 9 at 44-46 describing what a digital signature is, how electronic communications are digitally signed, and what the pre-requisites for the use of a digital signature are.

[55] *See: Ibid.* describing the RSA authentication process as follows: "suppose Alice wants to send a signed document m to Bob. Alice creates a digital signature s by exponentiating: s = m^d mod n, where d and n belong to Alice's key pair. She sends s and m to Bob. To verify the signature, Bob exponentiates and checks that the message m is recovered: m = s^e mod n, where e and n belong to Alice's public key... Anyone can send or verify a signed message, using only public keys, but only someone in possession of the correct private key can decrypt or sign a message."

signature. The sender then attaches the digital signature to the communication and sends both to the intended recipient."[56] The integrity of the message is verified through the use of the corresponding public key.

Authentication protocols, however, can be based on either conventional secret-key systems or on public-key systems. In this latter case, authentication uses digital signatures.

Since *secure* digital signatures cannot be forged, the signer of a message cannot later repudiate it. This is known as the "non-repudiation" feature of digital signatures.

To sum up, digital signatures used alone do not provide any security as to the confidentiality of the signed message; they only provide security as to the integrity, authenticity, and non-repudiation of the message. Therefore, the communication must be encrypted in order to ensure its confidentiality, but an encrypted communication can also be digitally signed.

Digital signature systems must be supported not only by a strong cryptographic technology, but also by institutional and legal infrastructures. Cryptographic technologies are already available in the USA and Canada to complement digital signatures, for instance with encryption and date/time stamping utilities. The institutional infrastructure, which includes governmental and private entities, is now operating in these two countries too. The legal infrastructure for digital signatures is beginning to be developed. Utah[57] and California[58] have passed, to date, digital signature legislation. The core of the Institutional infrastructure required by digital signatures is the body of Trusted Third Parties [hereinafter TTPs], also called

[56] *See: Ibid.*, at 45. *See also:* M. S. Baum. *"Digital Signature Primer in Verisign, Inc."* Frequently Asked Questions Appendix 1 (June 23rd., 1995). Available online at URL http://www.verisign.com/faq.

[57] Utah Code Ann. S. 46-3-101 *et seq.* (eff. May 1, 1995)

[58] California Government Code. S 16.5 (Enacted Oct. 4, 1995).

Certification Authorities.[59]

Some legal aspects about Trusted Third Parties.

The advantages of digitally signing messages are numerous, as we described above. But if digital signatures are to be reliable, so must be the TTPs.[60] Their role is critical: to ascertain the identity of the subjects on all digitally signed communications.[61] How can this be done? By certifying the existing association or connection between a determined pair of keys (public/private) and a certain person (the subscriber).

When a subscriber approaches the TTP for certification purposes, the TTP must ascertain two things: the identity of the subscriber,[62] and the fact that he/she has the private key that corresponds to his/her private key. Note that it is not necessary at all for the subscriber to disclose the private key. Once the TTP has certified that the association between a subscriber and the key pair he/she possesses exists, it must issue a certificate. This certificate is a digital document whose integrity and authenticity must be guaranteed by the TTP as well. The way of doing it is by digitally signing the certificate record.

[59] In this study, we only outline some basic Certification topics. They deserve a separate investigation. For further reference on these topics *see*: T. J. Smedinghoff. *Supra*, note 9 at 47-53. *See also*: P. Fahn. *Supra*, note 44.

[60] "[A] digital signature is only as reliable as the certification authority is in performing its functions." *See*: Smedinghoff. *Ibid.*, at 49. The author also describes the way to gauge the degree of trust one should place on a TTP, called *certification practice statement*.

[61] *See, e.g.*: B. W. McConnell, E. J. Appel & Co-Chairs, Interagency Working Group on Cryptography Policy. *"Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure."* Executive Office of the President, Office of Management and Budget, Washington, D.C. May 20, 1996 Available online at URL: http://www.isse.gmu.edu/~pfarrell/NIST/kmi.html, discussing thoroughly the Key Management Infrastructure [hereinafter KMI] surrounding the Certification authorities' role in escrow systems.

[62] *See:* M. S. Baum. *Supra*, note 56, stating that Verisign, Inc., relies on notaries in order to verify the association between a subscriber and a determined pair of keys.

The TTP then notifies the subscriber that it has issued a certificate that corresponds to him/her. The subscriber will have to verify the accuracy of the certificate because it signifies that he/she is prevented from repudiating the communication or his/her sending the message. Any communication sent with the subscriber's private key will bound him/her. Once the contents of the certificate have been verified, it can be published[63] either by the subscriber or, under his/her request, by the TTP. If the subscriber does not want to be bound anymore by his/her digital signatures, he/she will have to revoke his/her public key.

[63] This means to make it available to people who wants to communicate with that subscriber.

CHAPTER II. ENCRYPTION LAW IN OTHER COUNTRIES

1. The US Data Encryption Standard.

2. The US Escrow Encryption Standard and the Clipper Chip.

3. Overview of Cryptographic Products Export Controls in the USA The International Traffic in Arms Regulations, and the Arms Export Control Act.

A) ITAR's exemption for personal use.

B) The key-length.

C) Encryption cases.

i) The Zimmermann case.

- *The personal and commercial approaches.*
- *The legal approach.*
- *The fair-competence issue .*
- *The free-speech issue .*

ii) The Bernstein case.

iii) The Karn-Schneier case.

D) "Pro-Net" security Bills: some legislative examples of encryption.

i) The Encrypted Communications Privacy Act.

ii) The Promotion of Commerce Online in the Digital Era Bill.

iii) The Security And Freedom through Encryption Act.

4. Overview of the French Encryption Import Controls.

5. Overview of the Russian and the Japanese encryption legislation.

- *Russian Federation's approach to encryption.*
- *Japan's approach to encryption.*

6. The Meeting of Experts on cryptography. Towards a global escrow system?

CHAPTER II. ENCRYPTION LAW IN OTHER COUNTRIES.

Encryption technologies ensure the privacy of personal, commercial and governmental data in electronic storage. There are several encryption "levels", depending on the algorithm the system uses and the key length it provides.[64]

There are some problems that law around the world faces with the spread of encryption technologies.[65] Governments have difficulties defining to what extent encryption is a good tool for protection of individual and commercial privacy, and to what extent it becomes a problem for law enforcement. They have difficulties even defining what encryption *is*. For some countries, strong encryption technologies are munitions that should be controlled for export[66] or import.

The comparative bases used here encompass a variety of

[64] For the purposes of this study, the term "strong" encryption refers to encryption systems that use a key bigger than 56 bits. *See*: M. Blaze *et al.* *"Minimal Key Lengths For Symmetric Ciphers To Provide Adequate Commercial Security."* Jan., 1996. Available online at URL http://www.bsa.org/bsa/cryptologists.html The authors explain the different key lengths that are necessary for a maximum protection degree for each different user. For instance, they argue that at least a 75 bit key is necessary to protect commercial enterprises' information. To protect information over the next twenty years the key should be 90 bits long.

[65] *See* the exhaustive study of J. P. Chandler *"Identification and Analysis of Foreign Laws Pertaining the Use of Commercial Encryption Products."* (Washington, National Intellectual Property Law Institute and George Washington University. Jan., 1994). Available online at URL: http://www.sevenlocks.com/papers/crypto/lawfor.txt. The author studies import and export control laws to encryption products worldwide.

[66] For instance, *see*: *infra*, Chapter II, part 3, when we discuss encryption export restriction in the USA.

perspectives: the US Data Encryption Standard, the US Escrow Encryption Standard, the US export controls, and the French, Japanese and Russian encryption laws.

The US Data Encryption Standard is described as one of the first attempts to standarize the use of encryption in that country. It represents a good example of how a standard becomes increasingly vulnerable and thus dangerous.

The Escrow Encryption Standard is the most recent attempt by the US Government to establish a system that provides great searching abilities for the government. As such, it has been controversial. Its study is important since it helps us describe the debate occurring between civil libertarians and the government.

We then examine the US International Traffic in Arms Regulations and study whether they have accomplished their objectives. Farther on, we analyze the most relevant encryption cases and the legislative examples on encryption that have emerged as a response to these Regulations.

The French and Russian legislation represent some of the most strict systems in the world regarding encryption. The Japanese, on the other hand, do not worry too much about the potential dangers of strong encryption. They are more preoccupied in making good use of encryption for international trade.

Finally, we examine the OECD's Meeting of experts on cryptography, and its interest on escrow systems. We then draw some conclusions from it that represent the first steps towards a global encryption regulation.

1. The US Data Encryption Standard

In the 1970's, the National Institute of Standards and Technology [hereinafter NIST] -then called the National Bureau of Standards [hereinafter NBS]- decided to establish a cryptographic national standard. One of the reasons for this was the interoperability problems that emerged because of the inability for the different cryptographic products used at the time to communicate with each other. In 1977 the NBS chose an algorithm developed by IBM, which became the US Data Encryption Standard. The first key used by the DES was twice the size of the final key.[67] This fact gave raise to fears that the key-length became shorter to make it easier for the NSA to break it and that perhaps there was an implanted weakness (or "back door") that would allow the Agency to break the code by shortcuts.[68]

Even though DES is one of the most widely used cryptosystems in the world, it has been found to be vulnerable to brute-force attacks.[69] This algorithm uses single-key technology[70] which results in key-management problems.[71] It is also dated and increasingly vulnerable.[72]

The risk of using short keys is critical. Recently, for instance, two French graduate students successfully attacked Netscape's 40-

[67] The former version of the DES used a 112-bit key, and the latter a 56-bit key. See: B. Schneier. *Supra*, note 41 at 221.

[68] *Ibid.*, at 224.

[69] *See generally* G. Garon & R. Outerbridge, *"DES Watch: An Examination of the Sufficiency of the Data Encryption Standard for Financial Institution Information Security in the 1990's"*, [1991] Cryptologia, at 177.

[70] See *supra*, Chapter I, part 3, section C), subsection i).

[71] For a comprehensive discussion of Key Management issues *see:* B. W. McConnell *et al. Supra*, note 61. *See also* the key management problems in connection with single key technology, *supra*, Chapter i, part 3, section A), subsection i).

[72] *See*: M. Blaze *et al. Supra*, note 64. The study states that 40-bit key lengths, such as DES', offer virtually no protection, and that even DES with 56-bit keys (which is used for some commercial purposes) is increasingly inadequate.

bit algorithm using their school's computing facilities. "There is no need to have the resources of an institution of higher education at hand, however. Anyone with a modicum of computer expertise and a few hundred dollars would be able to attack 40-bit encryption much faster."[73]

There are some possibilities to achieve better security besides DES. Either using "triple DES",[74] changing DES keys often,[75] or replacing DES completely or partially will suffice.[76]

This issue has not been clarified yet. The US Government has proposed the Escrow Encryption Standard in an attempt of achieving better security for personal privacy, but making it possible for the US law enforcement authorities to intervene in communications, as analyzed next.

There are important lessons we can draw from DES: first, it is very positive that people and their governments reach a consensus as to whether or not a standard is the best solution to data security concerns. Second, both governments and people must be aware of the dangers of encryption systems becoming vulnerable and, by consensus too, must achieve a balance that allows the maximum degree of personal and commercial privacy, without threating law enforcement activities. Third, the role of the governments as promoters of technological advances on communication security is decisive in the process of achieving that balance.

[73] *See: Ibid.* The authors estimate that for about $400 anybody possessing some computational skills could recover a 40-bit key in an average of five hours. "The bottom line is that DES is cheaper and easier to break than many believe."

[74] This means processing the message three times with DES. This can be problematic because it requires encrypting the message, then decrypting it with a different key, and then re-encrypting it. The second disadvantage is a loss in speed and, most importantly, the uncertainty of its safety because the NSA has not stated yet whether triple-DES is secure or not.

[75] But besides the above mentioned key-management problem, this solution would not work for things that have to be kept in secret for long periods of time.

[76] If DES were to be replaced partially, it could be possible to use public-key cryptography in the frequent exchange of keys only. This would probably lead to the absolute replacement of DES in the short run because it would mean setting DES to a more secure system to complement its "weaknesses".

2. The US Escrow Encryption Standard and the Clipper Chip.

The Escrow Encryption Standard [EES][77] emerged as a result of the US Government's concern about the eventual substitution of DES. The Government proposed this system in part because it would enable it to keep some kind of control, by holding a copy of all EES keys needed to decrypt communications using this system. The Government argues that EES would represent a good tool in crime detection by the US Federal Bureau of Investigation [FBI] and law enforcement.[78] There are many important legal outcomes if the EES became effective as the only encrytpion standard. Let us first examine in greater detail how EES works.

The US Government has promoted the use of the EES to be implemented in the "Clipper Chip" and other devices,[79] to ensure the "wiretapping and electronic espionage capabilities that it has enjoyed since soon after the invention of the telegraph and the telephone."[80] The Government's proposal is to provide a strong encryption technology for the public, certified by the National Security Agency as unbreakable for many years. In exchange, the

[77] Also known as "Clipper Chip", in the case of telephone chips, and as "Capstone Chip" and "Fortezza" PCMCIA Card for message exchange. EES technology uses a 80 bit key length, which is considered by experts to be appropriate and secure enough. *See*: M. Blaze *et al. Supra*, note 64.

[78] *See generally*: S. A. Baker. *"Don't Worry, Be Happy: Why Clipper Is Good For You,"* [1994] Wired.

[79] Such as the "Capstone Chip", which is designed to be used in electronic mail, digital signatures, etc. *See generally*: National Institute of Standards and Technology, *Capstone Chip Technology*, (Apr. 30, 1993), in L. J. Hoffmann, ed. *Building In Big Brother: The Cryptographic Policy Debate*. Mar. 1995, at 413.

[80] *See*: M. A. Froomkin. *Supra*, note 15 at 715

Government will keep its ability to intercept or read encrypted information, by keeping a copy of the keys.

Mandatory key escrow, we believe, would infringe personal privacy[81] and reduce associational freedom.

The EES system consists in a chip that has a unique serial number and a corresponding single-encryption key [hereinafter the *chip key*][82] that is split in two parts. Each of these two pieces is retained by a different "escrow agent".[83] The Government can require both agents to release the segments of the chip key, and then reunite them in order to intercept communications, if there is a legally valid reason for doing so.[84]

To start an encrypted communication between two clipper-equipped telephones,[85] the user "X" will have to push the security button and wait until his/her telephone and "Y's" telephone are synchronized and the security of the conversation ensured. The conversation that follows will be then scrambled with an algorithm

[81] For a comprehensive description of some privacy topics under the U.S. laws *see:* R. Lance. Supra, note 6, at c. 5, p. 165-185. The author describes encryption as a self-help privacy measure, at 181.

[82] Chip key can either mean one of the two parties of the hardware component needed to decrypt "clipper chip" encrypted data, or the equivalent software information needed to decrypt "capstone chip" encrypted data.

[83] The proposed escrow agents were the Department of Commerce's NIST and the Treasury Department's Automated Systems Division (*i.e.*, the Government itself). *See*: U.S. Department of Justice, *"Attorney General Makes Key Escrow Encryption Announcements"* 2 (February 4th., 1994), at 1, *in:* Office of the Press Secretary, The White House, *"Key Escrow Encryption: Announcements"*-February 4th., 1994 (February 15, 1994). *See also*: S. McLandish, responding to Dorothy Denning's *The Future of Cryptography*, available online at http://www.eff.org/pub/Crypto/ITAR_export/Key_escrow/denning_02. "However, due to an icy reception, the Administration altered the proposal allowing for commercial non-governmental key escrow agents. This would still allow government access to keys through a warrant. This new proposal has been dubbed Clipper II." *See*: (Anonymous) *"Encryption: A Free Society's Dilemma: A Discussion of Legislative Proposals to Regulate the Use and Export of Encryption Technology."*. Available online at URL http://www.law.miami.edu/~froomkin/ seminar/papers/anon/intlaw-paper.html, at 2.

[84] "The point is that ultimately no message encrypted by Clipper is safe from the Government." R. Lance. *Supra*, note 6 at 170.

[85] For an excellent description on how does clipper work, *see*: M. A. Froomkin. *Supra*, note 15 at 752 through 759.

called "Skipjack",[86] which is classified and certified by the NSA as secure. The communication is encrypted with a specific *session key.*. This session key is only used for that single transmission of data, *i.e.*, each conversation will have a new session key and no conversation will be possibly decrypted without its corresponding session key. The session key is encrypted by each of the two phones with the chip's key. Each Clipper Chip has its own chip key.[87] The next step is to attach the sending chip's serial number and a *checksum*[88] to the whole "message package", which is finally encrypted with a third key: the *family key.* This family key is shared by all chips, and is held by the Government.

When beginning any Clipper conversation, "X's" Clipper Chip sends a Law Enforcement Access Field [hereinafter LEAF] to "Y's" Clipper, and without a valid LEAF for the recipient's chip, there will be no communication.

To summarize, there are three keys: the session key (which encrypts the conversation with the Skipjack algorithm, and is special to each conversation); the chip's key (which encrypts the session key and is different from one chip to another); and the family key (which makes a final encryption of the chip's key, the checksum, and the chip serial number). The family key is common to all chips and is the key that the Government keeps.

In order for the Government to decrypt a message, it must first intercept the message that includes the LEAF. Then it must decrypt the LEAF with the family key. Then, it must speak to the

[86] For a description of the algorithm and a statement about its security, *see*: E. F. Brickell *et al.* *"SKIPJACK Review Interim Report: The SKIPJACK algorithm ."* (July 28th., 1993). Available online at URL http://www.quadralay.com/www/crypt/clipper/Skipjack-review.html.

[87] These are the keys that are split between the escrow agents and are indexed by the chip's unique serial number.

[88] This checksum, also called "hash value", is the product of a "hash function". A hash function consists in taking "a variable-length and convert[ing] it to a fixed-length string of characters," which is then called checksum or hash value. *See:* T. J. Smedinghoff. *Supra*, note 9, at 501-502, summarizing hash function's operation.

escrow agents to request from each of them the segments of the chip's key, if there exists a legal justification for the "wiretap." Once the two chip key segments are together they produce the chip key itself. The session key can be revealed, by decrypting it with the chip key, and the message can be finally accessed using the corresponding session key.

The escrow agents have a critical role to play here because they will create and hold the segments of each different EES key and thus will participate in the creation of each chip key. They will keep the number that consists in half the information that is needed to recreate a chip's key. They will also have to keep a detailed record of requests over key segments.

The *Capstone Chip*[89] system (and the *Fortezza card*) works mostly in the same way, but with one difference: the session keys are encrypted with public-key encryption. When the Government wants to decrypt these kinds of messages, it will need to decrypt the LEAF with the family key. Then it will request from the escrow agents their correspondent parts of the chip's key (which consists in everybody's private keys, but split in two).

The major disadvantage of this situation is that the Government will require the chip key of every person who has contact with the person whose conversations are being wiretapped. Thus, it will collect a large number of valuable chip keys that belong to people who are not under investigation.

Although technically the EES system seems to be "secure" enough for users (because of the protection it provides against third parties in general), there are very important concerns about lacks in "legal guarantees for the people whose keys are generated by the Government and held by the escrow agents. [In cases of illegal

[89] The Capstone Chip is the correspondent EES version of the Clipper Chip for e-mail. This technology provides also digital signature advantages and, since this is not a way of storing or keeping information safe, the system is supposed to allow users to change the digital signature password.

wiretap, there] appears to be no remedy against the escrow agents, even if the escrow agents acted negligently or failed to follow their own procedures."[90] However, the regulations concerning the work of the escrow agents can still be changed, waived or amended at any time. There is still the worry about the permanent status of the escrow agents: because they possess such a high valued information, they will always have to be trusted. Otherwise, they will not be able to participate in the EES progress.

The US Government hopes that EES will become a de facto market standard. Nevertheless, EES seems unlikely to displace other types of cryptography (such as public key cryptography), that do not contemplate the Government's chance of having the keys from the beginning, even though there is a valid concern about some arguments of protecting national security.

The US Government realized this situation and proposed what is known as "Clipper II" and "Clipper III" initiatives. The change that the US Administration made about the proposed escrow agents is what is known as Clipper II. Originally, the Government proposed two Governmental Agencies to function as the escrow agents, as mentioned before.[91] Due to a negative reception, it changed its criterion to allow commercial non-governmental entities to function as escrow agents.

Clipper II has not suggested further substantial changes, compared to the original Clipper project, so all the comments made about Clipper are also valid here. The escrow continues to give the government the possibility of keeping the family key and requiring the production of the two parts of the key from the escrow agents.

Under Clipper II the Government was still in charge of determining the conditions for the escrow, and this is one of the

[90] M. A. Froomkin. *Supra*, note 15 at 762.

[91] *I.e.*, the Department of Commerce's NIST and the Treasury Department's Automated Systems Division.

reasons why,[92] just like the Clipper I original project, Clipper II did not succeed. Other reasons may be that Clipper II was optional, and therefore people choose other non-escrowed encryption technologies.

Clipper III was the name people gave to the US initiative to create a sort of international escrow standard. An International Key Management Infrastructure [hereinafter KMI) was proposed. The reaction to this initiative by the Internet community has been to create the "Internet Privacy Coalition", which has been giving support to legislative efforts to stop escrow initiatives,[93] such as the Encrypted Communications Privacy Act, the Promotion of Commerce Online in the Digital Era Bill, and the Security And Freedom through Encryption Act.

3. Overview of Cryptographic Products Export Controls In the US

In the USA, the export of encryption technology is restricted: it requires explicit authorization from the Government. In general, "[t]he US government has historically been reluctant to grant export licenses for encryption products stronger than some basic level (not publicly stated)."[94]

The Commerce Department and the State Department have adopted regulations that restrict the export of encryption

[92] *See: La loi sur les télécoms met l'Internet en laisse.* Bulletin lambda 2.08. June 10th., 1996. Available online at URL http://www.freenix.fr/netizen/208. html.

[93] *See:* M. A. Froomkin. *Supra,* note 15 at 762.

[94] *See:* P. Fahn. *Supra,* note 44.

technology. The two main sets of US regulations that govern the export controls in cryptographic products[95] are: the Commerce Department Export Administration Regulations [hereinafter EAR][96] and the International Traffic in Arms Regulations [hereinafter ITAR],[97] which implement the EAR.

The EAR control the export of goods and information "and know-how, whether in tangible or intangible form, that can be used to manufacture, utilize or reconstruct goods, including computer software and technical data. However, the export of some forms of software and information, particularly those involving encryption, may also be controlled by the ITAR."[98]

[95] US export controls in cryptographic products have mainly the following *purposes*: 1. To limit foreign availability of cryptographic systems capable of resisting concerted cryptanalytic attack; 2. To limit foreign availability of cryptographic systems of sufficient strength to interfere with traffic selection. *See*: S. Landau *et al*. *Codes, Keys and Conflicts: Issues in U.S. Crypto Policy*. Discrete Mathematics Seminar. (Rutgers University, Feb. 16th, 1995), at 25. Abstract available online at URL: http://dimcsa.rutgers.edu/events/titles/landau.html.

[96] Under the Export Administration Act of 1979, as amended by the Export Administration Amendments Act of 1985 (50 U.S.C. App. 2401-2420) and the EAR (15 C.F.R. ss. 768-799), the export of virtually all goods, software, technology and data is regulated by the Commerce Department.

[97] In the present study, we do not discuss free speech issues under ITAR. For reference on this topic see: M. M. Cleh, *"Government Control of Private Ideas-Striking a balance Between Scientific Freedom and National Security."* (1982) Jurimetrics Journal. No. 1, 22.

[98] *See:* Smedinghoff, T. *Supra*, note 9, at 397-398. The ITAR are available at 22 C.F.R. Parts 120 *et seq.* (1994). Statutory authority for the ITAR is the Arms Export Control Act, codified as amended at 22 U.S.C. Sec. 2778 (1988 & Supp. IV 1992). The ITAR define cryptographic devices as munitions, *see*: 121.1 (b)(1)(ii) regulates "the automation of munitions control functions and the processing of munitions control license applications, including the development, procurement, and utilization of computer equipment and related software."

As opposed to the EAR, the ITAR are applied by the State Department. The ITAR regulate, in general, the export of "defense articles" (*see: ibid.* at s. 120.1(a) and 120.6, which define what the term defense article means, and mention military equipment, firearms, guidance and control equipment) and the "technical data" to design, develop, manufacture or operate those articles (*see: ibid.* at s. 120.10). Export is construed not only as any transmission of the restricted products out of the US, but also as any disclosure to a foreign national, "even if the foreign national is in the United States." *See*: Smedinghoff, T. J. *Supra*, note 9, at 398. Civil penalties for failure to comply with the export regulations can reach $100,000 per transaction, and for criminal violations fines can reach $250,000 plus 10 years in prison (*see*: 50 U.S.C. App. ss 2410 (a)-(c)).

US encryption law and policy have been extensively debated over the past three or four years. Within this process, there have been important privacy concerns. On the one hand, civil libertarians have been mostly concerned about cryptographic security measures. On the other hand, the US Government has been worried about national security protection and law enforcement. The EES came to fuel this debate[99] between civil libertarians and national security concerns for several reasons. First, it was considered as mandatory in the original proposal. Second, EES products are the only encryption product free of complying with ITAR export controls and, thus, will become the only exportable strong encryption product in the US.[100]

Have the US encryption export controls achieved their goal? Not really. Cryptographic controls have been particularly unsuccessful in stopping the spread of cryptographic products outside the USA.[101] Current spread of strong cryptographic products worldwide, such as DES-based products or the military-grade PGP, evidence that the ITAR have failed to prevent the availability of these products outside the US, and its enforcement has sometimes even produced some absurd results.[102]

DES is used worldwide and incorporated in different softwares. Yet, current US Government policy often limits the export of encryption software or hardware that incorporate algorithms using 40-bit keys. Export of other algorithms and key lengths must be reviewed on a case by case basis. DES with a 56-bit key, for instance, has been approved for export for specific purposes, such as financial transactions.[103] "Although US law ordinarily prevents

[99] *See:* M. A. Froomkin. *Supra*, note 15 at 743-744.

[100] Whether or not this will constitute an unfair treatment that will gave rise to valid claims from disadvantaged competitors, is out of the scope of this work.

[101] *See*: M. A. Froomkin. *Supra*, note 15 at 748-752.

[102] *Ibid.* at 750-751, and *see* the Karn case comments, *infra* Chapter II, part 3, section C), subsection iii). For the case reference *see infra*, note 117.

[103] *See*: M. Blaze, *et al. Supra*, note 64.

Americans from selling DES-equipped encryption products to foreigners, DES is found around the world and freely sold by foreign corporations in many countries."[104] Generally, some European and other countries that export DES-based software to the USA treat these exports more liberally than the United States treats DES exports to those countries. DES is sometimes the national standard abroad.[105]

As to EES, there are many unsolved issues yet.[106] A very interesting area of concern is the EES marketing possibilities in foreign countries. It will be the first freely exportable encryption product.

Obviously, one of the main concerns of foreign countries is whether or not they should buy an encryption product that gives the US Government the possibility to decrypt all the data encrypted using EES. If they so choose, they might ask whether they should request the right to know the family key or accept to leave it only in the hands of the US Government and, in case of an investigation, work on a case-by-case basis. To give a foreign country Government the family key weakens the security level that the EES should offer. It also creates the problem of deciding[107] the most suitable key

[104] M. A. Froomkin. *Supra*, note 15, at 737.

[105] *See*: B. W. McConnell *et al*, *supra*, note 61.

[106] M. A. Froomkin. *Supra*, note 15, at 786, discussing the unsolved issues regarding the Clipper Chip proposal.

[107] *See*: B. W. McConnell *et al.*, *supra*, note 61. The Authors stress the need to establish an escrow policy over cryptographic keys "which provides a basis for bilateral and multilateral Government agreements... so that industry can produce products for worldwide inter-operability." The goal of this proposal is to create escrow encryption products "which will assure timely, lawful, Government decryption access." This proposal, thus, seems to add almost nothing since the Clipper Chip is a strong product which is secure enough against third parties' attacks.

We found an interesting concern on this document, though. It refers to the risk of proliferation of cryptographic products. The problem with this is the key recovery in case a key is lost, stolen, or forgotten because encrypted data would become useless. Luckily, today most public-key systems provide safety in this issue. In this study, we do not get into detail of this topic. For reference *see*: P.

management system for both the foreign country and the USA in order to preserve the EES level of security, the relationships between Governments, and the rights of the people under investigation or wiretapping.

There is also the chance of granting the foreign country Government the possibility of keeping the keys of those chips given to it (*i.e.*, the Government could then decide on its own national escrow agents), and producing different families chips, each one for a different market.[108] However, it seems unlikely since foreign Governments may not accept to buy an encryption product for which the US Government already has the keys. Moreover, it seems unlikely that the USA will sell EES products without retaining somehow the controls that motivated the creation of the standard.

There are many issues which are still under consideration. Export controls in the USA and other countries are frequently discussed. The result of this discussion is at times satisfactory, such as in the case of the ITAR's exemption for personal use which has been recently released, and which is discussed next. However, no result will ever please everybody.

The most important thing in cryptographic export controls policy is to try to achieve a balance between personal privacy and law enforcement requirements. In order to obtain this balance, however, countries and their societies have to deal with frictions. For instance: how long does a key need to be in order to be secure? What does national security mean? Is it a valid argument? What parameters are going to shape future legislation on encryption?

Fahn. *Supra*, note 44. *See also*: *Administration Statement on Commercial Encryption Policy*. Executive Office of the President, Washington, D.C. (July 12th., 1996). Available online at URL http://csrc.hcsl.nist.gov/keyescrow/admin.txt, stressing that "[t]he Clinton Administration is proposing a framework that will encourage the use of strong encryption in commerce and private communications while protecting the public safety and national security. It would be developed by industry and will be available for both domestic and international use."

[108] *See*: M. A. Froomkin. *Supra*, note 15 at 787.

i) ITAR's exemption for personal use.

On February 16th, 1996, the ITAR have been amended[109] by establishing an exemption for the temporary export of cryptographic products for personal use. The Department of State passed the reform to ease the burden on US citizens and lawful permanent residents who temporarily leave the USA carrying with them cryptographic products for their personal security abroad.

The exemption has, however, some limitations. For instance: it does not apply if the person contemplates sales, marketing or demonstration of the cryptographic products he/she carries. Moreover, the exemption does not apply to exports to certain destinations, which are listed in Section 126.1 of the ITAR. Those destinations are "countries that have been determined to have repeatedly provided support for acts of international terrorism, *i.e.*, Cuba, Iran, Iraq, Libya, North Korea, Sudan and Syria."[110]

The exemption also sets out that the encryption product must remain in the possession of the exporter or another US citizen or lawful permanent resident traveling with him/her. A product is considered to be in the possession of the exporter "if the exporter takes normal precautions to ensure the security of the product by locking the product in a hotel room, safe, or other comparably secure location; and, while in transit, the exporter keeps the product in his/her carry-on luggage or locked in baggage accompanying the

[109] *See: Amendment to the International Traffic in Arms Regulations.* Federal Register Vol. 61, No. 33. Rules and Regulations. Department of State, 22 CFR Parts 123 and 126. February 16th., 1996. Available online at URL: http://www.law. Miami.edu/~froomkin/ persuse.htm.

[110] *Ibid.*

exporter which has been checked with the carrier."[111]

This exemption represents a recognition of the US Department of State of the inconvenience of treating a normal user of encryption as a "munition exporter" only because he/she wants to use an encryption system when traveling.

Finally, the exemption keeps the control scheme of the ITAR since the user can not sell, market or demonstrate the cryptographic product. Yet, there may emerge important concerns about the fact that the burden is now put on the user and his/her constitutional protections. It will still be problematic whether the injunction requiring the user to "demonstrate" normal precaution to keep the product secure limits the user's First Amendment protection of free speech.[112]

B) The key-length.

Encryption has an essential role to play in protecting the privacy of electronic information against threats from a variety of potential attackers.[113] Therefore, assessing the strength required for each different need (personal, commercial, governmental, etc.) is an essential step. The reason is that brute-force attacks against cryptographic systems once considered adequate are today both fast and cheap.[114]

The US Government restricts the export of strong encryption products. Strong encryption is not only achieved with a strong

[111] *Ibid.*

[112] *See*: the Bernstein case and its First Amendment implications, *infra*, Chapter II, part 3, section C), subsection ii)

[113] *See:* M. Blaze *et al. Supra*, note 64.

[114] *Ibid.*

algorithm, but also by the key-length. The Government has forbidden the export of keys bigger than 56 bits. Yet, anybody is free to use the key length of his/her choice.

There is the important question, however, of deciding how long a key should be in order to be secure.

One can say that the key size depends on the needs of the user, but who is to decide what is necessary or enough for everybody? There is no absolute answer to this question, but there are some guidelines that future policy making on encryption can take into account.

For instance, the study of Blaze *et al.*[115] gives expert guidelines on the key length needed for every different purpose. This study concludes that as a result of the ease with which 40-bit key cryptosystems can be broken, they offer virtually no protection against serious attacks (such as by big commercial enterprises or government intelligence agencies), and should be substituted for strong encryption systems since the cost is not significantly greater than that of weak encryption. The study recommends the use of 75-bit keys, or 90-bit keys to adequately protect information for the next 20 years "in the face of expected advances in computing power".[116]

Our opinion is that the key size should be left to the free choice of the user.

[115] *Ibid.* The recommendations indicated in this study are to provide maximum protection against Government intelligence agencies and industrial espionage.

[116] *Ibid.*

C) Encryption cases.

There are three main cases that have dealt with encryption in the USA. The first was the Zimmermann case (the author of PGP), which raised important questions, even though it ended with the mere investigation of Zimmermann. Recently, two other cases emerged and brought the issue of encryption to US courts: Karn v. US Department of State,[117] and Bernstein v. US Department of State.[118]

All cases are helpful in defining constitutional implications of the use of encryption, which shape encryption legislation.

i) The Zimmermann case.

PGP's author Philip R. Zimmermann was criminally investigated[119] by the FBI for violating the ITAR because PGP was

[117] *See:* Karn v. United States Department of State (D.C. Cir. 1996), available online at URL http://www.qualcomm.com/people/pkarn/export/decision. html 960415.decision.

[118] *See:* Bernstein v. United States Department of State (Civil Action No. C9500582-MHP N.D. Cal. 1996). Available online at URL http://www.eff.org/pub/ Privacy/ITAR_export/Bernsteincase/Legal/960415.decision. *See also* a description of the case: *infra*, Chapter II, part 3, section C), subsection ii).

[119] Zimmermann was subject to investigation by the FBI since his release of PGP. In 1993, a Grand Jury in San Jose, California, was investigating charges against him for his "exporting" PGP. On November 9, 1994, Customs authorities detained him, searched his luggage and interrogated him about the itinerary he followed on the trip from which he was returning at that moment, his prior trips overseas, and possible PGP exports. Eventually he re-entered the USA.

On November 23, 1994 he took legal action, complaining about the incident and about the fact that the Customs authorities promised to follow the same procedures each time Zimmermann would leave the U.S. The case closed on January 1996. Today Zimmermann is no longer under investigation, and the FBI has dropped charges against him. For a description of the issue *See: Cryptography* considered a munition that should be subject to export controls. His violation was that he had "exported" PGP by making it available on the Internet.[120] Thus, the resulting debate concerning PGP's use between James Kallstrom, on behalf of the FBI, and Zimmermann, raised a number of interesting points concerning high-security softwares and national security issues.

PGP is the most-used e-mail encryption software around the world. One of the reasons for this is its high level of security: not even the FBI's intelligence services can break it, nor can super-computers. So, for personal and commercial uses, this privacy software is very reliable. Yet, for the FBI, such a high level of privacy can also be harmful in the hands of criminals. This is why PGP is considered a high-technology weapon.

PGP's author explains that most of today's communications are running over electronic channels, and that his creation is a social need: a guarantee of privacy on e-mail message transmission. He says that "[t]here's nothing wrong with asserting [one's] privacy"[121] by using encryption, a security measure equivalent to the envelope on conventional mail, so people can take "their privacy into their own hands".[122]

Do we have the right to protect our information from others' "looks"? On a simplistic view, the natural answer is yes. Everybody has to have a way to protect him or her self from others' observation. However, Kallstrom was worried about the fact that criminal investigation institutions could not detect criminal activities running over the Internet. The answer, then, is not so easy because we have to look very carefully at different perspectives of the

Export Control Archives, available online at URL http://www. *see also:* J. Markoff, *"Federal Inquiry on Software Examines Privacy Programs,"* New York Times, 21 September 1993, at C1. *See also:* J. Erickson, *"Cryptology Fires Up the Feds"*, [1993] Dr. Dobb's Journal, at 6.

[120] PGP is freely available online -for non commercial use- for Canadian and U.S. residents from ftp://rtfm.mit.edu.

[121] *See:* J. Erickson. *Supra,* note 119 at 5.

[122] *Ibid.,* at 6.

problem and the potential answers that may emerge from the different approaches: public policy, scientific, commercial, personal, and legal. There is a wide perspective on this topic, but no single comprehensive answer. The only vision that all levels share is that privacy is essential to communication, even if its limits are difficult to draw. Below we briefly discuss the main arguments of the Zimmermann-Kallstrom debate. Some aspects of this are worth taking into account for future encryption policy making in Mexico:

The personal and commercial approaches.

Personal and commercial levels of privacy have a deep reach. Almost all of today's transactions are conducted electronically. We pay via credit cards. The way of doing business is like this world wide: everything is made more and more "electronically comfortable". However, it is not electronically secure enough yet. The level of electronic comfort carries a high degree of risk and "privacy erosion."[123] Not using a security device or using an imperfect one is hazardous since either commercial entities or people can be subject to wiretapping, information interception or electronic espionage. Thus, if activities are not illegal, the use of encryption seem to be completely justified.

The legal approach.

In the US, strong encryption products are considered munitions and are, thus, subject to the International Traffic in Arms Regulations.[124]

[123] *"Power vs. Informatic Privacy: Debate Zimmermann-Kallstrom". La Jornada en Internet*, Virtualia Review no. 2, February 26th., 1996, available online at URL: http://serpiente.dgsca.unam.mx/Jornada.

[124] *See*: Supra, note 104. *See also: ITAR Export Restrictions.* Available online at URL http://www.eff.org/pub/crypto/ITAR/export/. *See also*: *Privacy - Crypto - ITAR Export Restrictions Archive*, available online at URL http://www.eff.org/pub/

Since strong encryption, and in this case PGP specifically, provides security to send or store information and encodes voice or data in a way almost impossible to break, the US Government worries about criminals using PGP. Kallstrom implied that the US Government wants to implement a method (the Clipper Chip) that makes law enforcement easier when prosecuting criminals who use encryption to their ends. Zimmermann explained that he created PGP as a response to the Government's Clipper Chip initiative because behind this idea was the possibility for the Government to intercept all encrypted information. For him, this represented a future deprived of privacy not only for criminals, but for everyone.

Kallstrom argued that such highly advanced encryption systems obstructed the proper operation of the US national security and intelligence agencies. Zimmermann used an example as an answer. He said that cars are used by everybody, even by criminals. This, however, is not a valid reason for the Government to be allowed to search everybody's cars. According to Zimmermann, solid encryption changes the relationship between people and their Government because strong encryption products allow secure information flow even through the Internet, leaving the user's personal data out of the governmental controls.

Kallstrom agreed that protecting information is positive for the good of the nation's trade, economy and international finances, and accepted that many things that can be used for opposing purposes. But Kallstrom claimed that people like Zimmermann could also help find a "master key" (to guess other's codes). Since a world wide encryption legislation control would be impossible to achieve, this master key, said Kallstrom, could help give a response to law enforcement problems connected with encryption, not only in the US, but also in the global context.

Privacy/ITAR_export/. The ITAR are administered by the Office of Defense Trade Controls in the Department of State.

The fair-competence issue.[125]

Since the US Government prohibited the exportation of programs that offer solid encryption, such as PGP, there have been several complaints, for instance from the computer industry and some financial entities. A problem highlighted by the computer industry is not only that they cannot sell encryption programs, but also that complete computer networks cannot be sold because they do not have a trustworthy security system.

The free-speech issue .

This is one of the most difficult topics that US courts have begun to face and many other courts in the world will encounter too. Two courts faced two important crossing points between encryption and freedom of speech. The first point refers to the encryption system as a language, and the criteria used to decide whether a technological creation such as that type of program should be considered speech or not. This question is addressed in the Bernstein case.[126] The other question refers to ciphered data, being the difficult question to decide whether a message that has been transformed by a hash function into cyphertext is a language or not.[127]

[125] For more information on this topic, *see*: U.S. Department of Commerce and the National Security Agency. *A Study Of The International Market For Computer Software With Encryption.* Document prepared for the Interagency Working Group on Encryption and Telecommunications Policy. Available online at: URL ftp://ftp. cygnus.com/pub/export/.

[126] *See:* Bernstein v. United States Department of State, *supra*, note 118.

[127] *See*: *infra*, Chapter III, part 3, section E), subsection iii).

ii) The Bernstein case

Daniel Bernstein developed a zero-delay public-key encryption system and described it in a paper entitled "The Snuffle Encryption System". He entitled the source code of the system "Snuffle.c" and "Unsnuffle.c." In June 1992, Bernstein asked the State Department to determine whether the three items were covered by ITAR. He obtained no response. In July 1993, Bernstein submitted a second jurisdiction request for his paper, "Snuffle.c" and "Unsnuffle.c", a description in English of how to use Snuffle, and instructions for programming a computer to use Snuffle.

The Office of Defense Trade Controls notified Bernstein (in October 1993), that all five items were subject to ITAR export restrictions. Bernstein filed a suit and only then did the Office clarify that its determination only applied to Snuffle.c and Unsnuffle.c.

Bernstein then sued the State Department for these restrictions on the grounds of unconstitutional restraints on speech, infringement of rights of association and equal protection, among other things.

The Government said that the source code's purpose was not communicative, but functional as a cryptographic product.[128] The court established that the encryption source code (the algorithm itself) was protected as "free speech" by the First Amendment. The rationale of the court was that even if the encryption source code was essentially functional, it may still be within the parameters of free speech. The Court stated that computer language communicates information in the same way that music or mathematical equations are speech. Furthermore, the court found "no meaningful difference between computer language,

[128] *I. e.*, that the algorithm itself *is **not*** speech, since it does not have the purpose of ***communicating*** any thing, but of accomplishing the ***function*** of ciphering the message.

particularly high-level [computer] languages ..., and German or French. All participate in a complex system of understood meanings within specific communities. Even the object code, which directly instructs the computer, operates as a 'language.' When the source code is converted into the object code 'language,' the object program still contains the text of the source program. The expression of ideas, commands, objectives and other contents of the source program are merely translated into machine-readable code."[129]

The Court concluded by emphasizing that the source code was indeed speech for First Amendment purposes.[130]

iii) The Karn-Schneier case

The Karn case did not deal with the free speech issue, addressed by the Bernstein court. The case rather focused on the standard applied in First Amendment cases with attention to what the State Department regulations addressed.

The court decided that the State Department's prohibition on export of a diskette that contained the same encryption information as a book was a "content-neutral" decision. The argument was that had the State Department decision been based on the contents of the source code, it would have violated the First Amendment. But, since the State Department decision was based on the *medium* to export the source code (the floppy disk) and not on the *content* of the source code (the algorithm), the court found no violation of the

[129] *See*: Bernstein v. U.S. *Supra*, note 118. *See also*: J. Rosenoer. "*Coded Speech*". Available online at: URL http://www.cyberlaw.com/cylw0396.html. Other files on the Bernstein case are available at URL http://www.eff.org/pub/privacy/ ITAR_export/bernstein_ case/.

[130] *See*: J. Rosenoer. *Ibid.*

First Amendment. Karn challenged the distinction between a disk[131] and a book[132] as an "arbitrary and capricious" administrative act.

The court was uncomfortable with the assumption that the source code in this case could be speech. Judge Richey pointed out on his judgment: "[t]he Court makes no ruling as to whether source codes, without the comments, fall within the protection of the First Amendment. Source codes are merely a means of commanding a computer to perform a function."[133]

The State Department's decision was based on an appreciation of the "means" and not of the "contents" of the items, as said above. Unfortunately, this situation eventually put the court's decision into an absurd situation because the State Department allowed the export of Bruce Schneier's book "Applied Cryptography", a paper-version of the information formerly contained in the floppy disk forbidden for export, even though the two items contained the same material. The spirit of the court's decision was not wrong, though: it tried to support the refusal to export the instructions to create a cryptographic software application contained in a floppy disk; to protect the source code itself was not its purpose.[134]

[131] *See*: Commodity Jurisdiction Case 081-94.

[132] *See*: Commodity Jurisdiction Case 038-94.

[133] *See*: Case #1:95CV01812 in the DC Federal District Court. September 21st., 1995.

[134] For a deeper discussion on the Bernstein and Karn cases, and a comparative study of the two decisions, *see*: M. Voorhees. "*A Tale of Two Crypto Court Cases Are Karn and Bernstein judges on the same planet?*" May 3rd., 1996. Available online at: URL http://www.infolawalert.com/stories/050396b.html. Other online files on the Karn case are available at URL http://www.qualcomm.com/people/pkarn/export/. *See also*: E. J. Radlo. "*Legal issues in cryptography*." (US: Fenwick & West. Jan., 1996), at 8 pointing out that "the Bernstein litigation, as well as the Karn litigation and the grass roots movement that sprang up surrounding the Zimmermann investigation, will not result in a complete elimination of the government's control of cryptography via the export laws, as the courts are reluctant to second-guess the Executive Branch in matters of national security. Rather, these cases will result in a liberalization of these laws by helping to focus political opposition to the government's policies."

Important conclusions can be drawn from these cases, which can inform the recommendations to the Committee for future encryption policy making in Mexico.

First, encryption use is completely justified to ensure communications privacy and protect information flow through risky environments.

Second, there is a debate concerning the use of strong cryptography since ciphered information is only understandable by the person to whom it is addressed. This may create some difficulties for law enforcement if cryptographic products are used to further crimes.

Third, there is another important debate concerning the nature of encryption. Should it be considered speech, a munition or simply a protection system. The same questions apply to whether encrypted information is speech. Both debates will necessarily have to be solved by either the Congress or the courts at some point.

Finally, concerning the export of encryption products, a recurring argument has been national security protection. Future encryption policies should carefully determine whether national security should establish controls over the exportation of strong cryptographic products and measure the extent to which these controls are effective. In Mexico, this process will have to involve the definition of national security since this is a vague idea today.

D) "Pro-Net" security Bills: some legislative examples of encryption.

Encryption export controls opened a debate that brought a series of important outcomes. The topic has raised crucial questions addressed to both the people and their Governments. For instance, what does the term "privacy" mean in connection with encryption? What is the extent to which the State can intervene in people's privacy? What are the valid reasons for doing so? How does the Government control the export of encryption products without damaging the domestic industry? Is encryption a term that means the same for everybody?[135]

In its first stages the debate over encryption use in the US was carried out between civil libertarians and the Government. Then, the computer industry joined the discussion. Now there is a new party, the US Congress. Important bills "have been introduced in order to attempt to regulate and more importantly deregulate, encryption."[136] The "Security and Freedom Through Encryption [hereinafter SAFE] Act" is one of these bills, which is being discussed in the House of Representatives.[137] The "Encrypted Communications Act of 1996" [hereinafter ECPA] and the Promotion of Commerce *Online* in the Digital Era" are bills being discussed in the Senate.[138]

In general, all these legislative efforts attempt to clarify several civil libertarian's concerns: first, that every citizen has the right to use the encryption program to protect security,

[135] For civil libertarians it may be a need of a basic right for protecting personal privacy. For the Government, if encryption is in the hands of the "wrong person", for the Government it may be a problem, a munition, an obstacle in law enforcement, etc. At the same time, the Government itself may be one of the most active users of strong encryption systems. Encryption will then be a need to protect diplomatic information, State secrets, etc. For the computer industry encryption may be a critical issue in fair competence, besides being a product that must be carefully handled. Thus, the way Governments handle encryption has a critical role to play in deciding what the impact on the society will be. This impact has too many facets that are difficult to predict and, once present, difficult to draw as well.

[136] *See*: (Anonymous) *Encryption: A Free Society's Dilemma*, *Supra*, note 83, at 2.

[137] HR 3011. 104th Cong. 2nd Sess. (1996). Pro-CODE and ECPA are available online at URL http://www.cdt.org/crypto/ or http://thomas.loc.gov. *See also*: (Anonymous) *Encryption: A Free Society's Dilemma*, *Supra*, note 83, at 2.

[138] S.1587. s. 104th Cong. Sess. (1996); and the Pro-CODE Act S. 1726 is 104th. Congress 2nd. Session, May 2nd., 1996. *See also*: *supra*, (Anonymous) *Encryption: A Free Society's Dilemma*, *Supra*, note 83, at 2.

confidentiality, and privacy of their lawful wire or electronic communications;[139] second, that the individual has the right to choose any available program, no matter the key length of it; third, that no one will be required to use a specific encryption system or to use any form of escrow.[140]

i) The Encrypted Communications Privacy Act

On March 5th., 1996, Senator Patrick Leahy (for the District of Vermont) introduced his bill into the Senate.[141] His introductory statement contained a number of interesting points. First, Senator Leahy focused on the bill's approach to encryption as the means to enhance online business, jobs in the computer industry, privacy, confidentiality, and security in electronic communications.[142] Second, the statement touched on a much debated issue: national security. Although the reference to this issue was short, it is significant that this is the only bill that mentions it. Neither the Pro-CODE, nor the SAFE do. In this regard, Senator Leahy's proposal was "to do a better job of balancing these concerns with American business' need for encryption and the economic opportunities for our high-tech industries that encryption technology provide."[143]

Still, they were a number of issues that the bill did not mention, which provoked an important reaction from Clipper Chip

[139] *See:* S.1587. *Ibid.*

[140] *Ibid.*

[141] *See: "Statement of Senator Patrick Leahy on Introduction of Encrypted Communications Privacy Act of 1996."* March 5th., 1996. Available online at URL http://www.cdt.org/crypto/leahy_stment.html.

[142] *Ibid.*

[143] *Ibid.*

supporters.[144]

For example, the bill ignored the two controversial issues of law enforcement and release of decryption keys. It did not report on whether or not the Fifth Amendment[145] protects individuals from the compelled production of keys[146] as well as on warrants for the delivery of private keys.

Despite its omissions, and besides the benefits for civil libertarians, the bill has positive aspects for Clipper supporters. First, under the terms of ECPA it is a crime to use encryption to commit a criminal act. Second, law enforcement authorities now have a statute to invoke when somebody uses encryption to hamper an investigation.[147]

Yet, decryption of files pursuant to a warrant is a topic which is not completely defined. In order to demand the decryption of his/her information from the supposed criminal, the government authority has to prove that offensive information that relates to that particular investigation was encrypted with the purpose of furthering the crime. The problem is the following: how the authority will make the connection between the crime and the encrypted information if it has no access to it?

We can conclude that decryption is one of the most difficult

[144] *See*, for instance, D. Denning, *"Letter to Senator Patrick Leahy."* March 14th., 1996. Available Online URL http://www.cdt.org/crypto/. This states that, since this bill would make it legal for everybody to use military-grade encryption, it would "erode" law enforcement's authorities' abilities.

[145] In the sense that the Fifth Amendment guarantees that "|n|o person... shall be compelled in any criminal case to be a witness against himself." *See*: U.S. Const. amend. V.

[146] For further reference on this topic *see*: *supra*, (Anonymous) *Encryption: A Free Society's Dilemma*, *Supra*, note 83, at 5. *See also*: People of the State of New York v. Leary, Part 72. January 8, 1996. (NY. App. Div. 1996). This case supported a motion to compel a man to provide a code for decrypting files suspected of containing bomb making information.

[147] *See*: Statement of Senator Patrick Leahy... *Supra*, note 141

challenges that any law related to encryption use regulation will have to face, not only in the USA, but worldwide. If law enforcement authorities had access to encrypted files almost at will, *i.e.* only justifying the mere possibility of crime commission, then a system like EES would be recommended.

If, on the other hand, one takes a more liberal approach and states that only criminals are ordered to decrypt information, we have several problems. First, what criminals will be subject to compulsory decryption? Second, how the connection will be made between information that is believed to be related to the crime if authorities can not validly or even possibly access it? Third, if authorities gained lawful access to the "suspected" criminal information, what parameters will determine the amount of the criminal's encrypted data -so only *incriminating* data (and not other private information)- should be decrypted? Finally, how are we going to deal with a situation where a criminal uses military-grade encryption that can not be disclosed in any other way than with his/her decryption key, with him/her refusing to do so?

The above mentioned topics present one of the most important challenges for encryption law at the moment. They are still unsolved but will surely make a difference between a law enforcement-freedom balanced scheme and one that is not.

Thus, the Mexican Committee has the important challenge of finding a balanced solution to advise the Mexican Congress. This solution should provide the maximum protection for privacy and at the same time not unduly inhibit law enforcement authorities on compulsory decryption in criminal cases.

ii) The Promotion of Commerce Online in the Digital Era Bill.

The introduction of Promotion of Commerce Online in the Digital Era [hereinafter Pro-CODE] bill to the US Senate was announced on March 28th., 1996, by Montana Senator Conrad Burns.[148] One of the purposes of the bill was to abandon systems proposed by the Government, such as EES, by restricting "the US Department of Commerce from imposing government encryption standards that were not: developed by the private sector, do not provide robust security, require people to relinquish control of a decryption key, do not have widespread commercial support and acceptance, do not provide for the ability to securely interact worldwide, and do not protect the privacy of users consistent with constitutional protections."[149] As for the ECPA, which was co-authored by Senator Burns and Senator Leahy, this proposal neither defined the extent of the term "constitutional protections",[150] nor did it mention the national security issue.

The Pro-CODE not only restricted the Government from controlling the export of encryption products, but it also allowed their export if comparable products are commercially available from foreign suppliers.[151] This situation afforded strong support for the bill from leading computing and engineering associations.[152]

[148] *See*: Press announcement of the Pro-CODE. "*Burns Has "CODE" for E-Commerce: Legislation Opens Internet for Commerce, Protects Intellectual Property.*" Available online at URL http://www.privacy.org/ipc/#resources/ burns/.

[149] *Ibid.*

[150] *See supra*, encryption cases, Chapter II, part 3, section C), subsections ii) and iii), exemplifying the existing problem between encryption and the First and Fifth Amendments.

[151] *See*: Press announcement of the Pro-CODE. *Supra*, note 148.

[152] *See*: Letter from Barbara Simons and Joel B. Snyder to Senator Burns, supporting the Pro-CODE, April 2nd., 1996. Available online at URL http://www. privacy.org/ipc/#resources/burns/, stating that "[t]he relaxation of export controls is of great economic importance to industry and users..."

The Pro-CODE Act of 1996 and the ECPA are very similar.[153] Pro-CODE does not contain any substantial difference to ECPA. Thus, the comments we made to ECPA are also valid with reference to Pro-CODE.

iii) The Security And Freedom through Encryption Act [154]

As mentioned before, all "Pro-NET" Bills share similar approaches. Under the terms of SAFE, as under ECPA and Pro-CODE, any person may use any encryption method of his/her choice, regardless of the encryption algorithm selected, the encryption key length chosen, or the implementation technique or medium used.

SAFE also prohibits the Federal and State powers to impose mandatory key escrow, but it establishes an exception: access for law enforcement purposes.

This Bill includes a part dealing with the unlawful use of encryption. "Any person who willfully uses encryption in furtherance of the commission of a criminal offense for which the person may be prosecuted in a court of competent jurisdiction [and] in the case of a first offense..., shall be imprisoned for not more than 5 years, or fined in the amount set forth in this title, or both; and... in the case of a second or subsequent offense..., shall be imprisoned for not more than 10 years, or fined in the amount set forth in this title, or

[153] *See: Open Letter to Internet Community From Senator Burns.* May 2nd., 1996. Available online at URL http://www. privacy.org/ipc/#resources/burns/. stating that the Pro-CODE "does not add any new criminal provisions and does not establish legal requirements for key-escrow agents."

[154] "Security and Freedom Through Encryption Act". Supra, note 137.

both."[155]

As regards exports of encryption, SAFE does not add much in comparison with ECPA. It only lists the items which will not require licenses for exportation.

As Pro-CODE, SAFE completely ignored the issue of national security. However, it added some criminal provisions. Under its terms, unlawful use of encryption in furtherance of a criminal act will be punished with prison for up to 5 years in the case of a first offense and up to 10 years in case of a second or further offenses.

4. Overview of the French Import Controls.

In this section, we briefly analyze the implications of article 12 of the French *Loi sur les Télécoms.*

The new text of this article nullifies certain procedures that previously existed before and required the authorization of the French Government to allow the private use of cryptographic systems that protected the integrity and confidentiality of messages.

France is one of the most distinguished countries in the world to severely block the private use of cryptographic measures for data security.[156] The Prime Minister Services Office [hereinafter

[155] *Ibid.* at Section 2, ß2804, subsections (a)(1) and (2).

[156] *See: La loi sur les télécoms met l'Internet en laisse. Supra,* note 92. Some even think that France is seriously considering mandatory key escrow. See: Steptoe & Johnson LLP. "*France's Proposed Statutory Trusted Third Party Rules for*

SCSSI] is the authority in charge of approving the use of encryption programs. Under the new conditions, the user of an encryption software or hardware must deposit a copy of his/her keys with a trusted third party, an authority which is independent of the State (in principle, but this is not determined yet). Law enforcement authorities may access the keys in case of investigation of the subject.[157]

Some people fear that the Trusted Third Party [hereinafter TTP] would be *Bertin*, an Industrial Engineering specialized Company that works on projects of High Strategic Technologies. Bertin has developed two single key cryptographic methods "Bleuet" and "Pétunia", whose algorithms are known by SCSSI and can thus be distributed in France. Pétunia can also be exported under license.[158]

Regarding import restrictions, France does not impose barriers to European products, but it does so to products coming from other countries.[159]

Article 28 of the Law No. 90-1170 on telecommunications regulation, dated December 29, 1990, contains several notable issues for our study.[160]

French restrictions mainly focus on controlling the entry of encryption products that provide confidentiality and privacy. Digital signature products are not so restricted.

The use of a secret coding method or service is freely allowed if the method or service can only be used to authenticate a communication or ensure the integrity of the transmitted message (*i.e.* if the method only consists of a digital signature and is not the

Encryption." Available online at http://www.us.net/~steptoe/france.htm. Other related URL links available in: Bortzmeyer, S. *L'utilisation du chiffrement en France.* Gopher://gopher.urec.fr/00/securite/ docs/lois/dssi_scssi. txt.

[157] *See: La loi sur les télécoms... Ibid.*

[158] What people fear is that in case *Bertin* becomes the certification authority, it would be the first French "electronic notary". *See*: *Ibid.*

[159] *France's Proposed Statutory... Supra,* note 156.

[160] *Ibid.*

cipher of the message). If the method ensures confidentiality and privacy, it is only approved if it uses coding conventions managed according to the conditions defined in Section II. Other cases require the authorization of the Prime Minister.[161]

Trading encryption products that ensure confidentiality with countries that do not belong to the European Community require prior authorization of the Prime Minister. In some cases this may require identification of the purchaser.

Failure to comply with those provisions, or violation of Section II, results in punishment that includes fines and imprisonment.[162]

To sum up, the French system presents a dichotomy that restricts the import and use of encryption technologies that protect or encode information, but allows the use of digital signatures (only implying authentication and integrity). This has an obvious reason: the French Government wants to keep the ability to decrypt any encrypted data almost at will. Even though the French is a system of key delivery to a certain TTP, and not properly escrow, its purposes are the same as under the EES. Thus, the comments previously made about escrow are also valid here.

French people (as almost anybody in the world with a computer and a modem) can have access to free strong cryptography on the Internet. This seems to render fruitless any law prohibiting the use or import of strong cryptography. Therefore, the French Government (and in general all governments tailoring an encryption policy) should seek an effective decryption system for criminal cases, that ensures access to encrypted data without undermining personal privacy.

[161] *Ibid.*

[162] *Ibid.*

5. Overview of the Russian and the Japanese encryption legislation.

Russian Federation's approach to encryption.

President Boris Yeltsin's Edict on "Measures to Observe the Law in Development, Production, Sale and Use of Encryption Devices and on Provision of Services in Encrypting Information" dated April 3rd., 1995, restricts the use, development, production, import and export of encryption technologies and other technological means that allow secure storage, processing and transmission of information.[163] These activities were previously under the exclusive control of the KGB, other national security agencies, and of the military.

Under the terms of the Edict, the Federal Agency of Government Telecommunications and Information [hereinafter FAGTI] attached to the Office of the Russian Federation [hereinafter RF] President is the authority responsible for reviewing the applications and issuing the licenses that relate to those restricted activities. FAGTI is also responsible for the security of government communications and for intelligence operations that involve encrypted and coded information.[164] In this way, the Edict prohibits "state organizations and enterprises from using in their information and telecommunications systems encryption devices, including cryptographic devices for providing authenticity of the information

[163] *See*: Steptoe & Johnson LLP. *Russian Statutes Restricting Use of Encryption Technologies*. Available online at: http://www.us.net/~steptoe/cyber.htm

[164] *Ibid.*, quoting art. 6. Law on Government Telecommunications, dated February 16th., 1995.

(electronic signature), as well as protected technological means for storing, processing and transmitting information which do not have a certificate of the Federal Agency of Government Telecommunications and Information attached to the Russian Federation President's Office."[165]

The import of encryption in the RF is also controlled. The authority in charge of restricting the import of unlicensed encryption products produced abroad is the Russian Federation State Customs Committee. In order to import a foreign encryption device, one must obtain a license from the Russian Federation Ministry of Foreign Economic Relations, which is issued after consultation with the Federal Agency of Government Telecommunications and Information attached to the Russian Federation President's Office.[166]

The Russian Federation seems to be very concerned with implementing these measures to, among other things, intensify the combat against organized crime. Some have expressed concerns about the new statutes seeking to revive and legitimize methods to control the Russian society.[167]

Again, the comments made concerning the EES and the French encryption systems are valid here. To impose compulsory escrow or other system that implies the delivery of the private keys to the governments or any TTP is to expose privacy to a high risk.

Japan's approach to encryption.

Japanese encryption legislation is taking a completely different approach on how to treat encryption from France, Russia and the USA.

The early stages of Japan's encryption policy making are

[165] *Ibid.*
[166] *Ibid.*
[167] *Ibid.*

showing that Japan wants to penetrate the Global Information Infrastructure treating cryptography as a national economic priority.[168]

In contrast to the United States and Europe, where law enforcement concerns play an important role in encryption policy, commercial interests predominate in Japan. National security concerns are not so important there, since the country has not had worries about encryption for almost fifty years. Besides, the Japanese police have very important political and constitutional limitations against wiretapping. Therefore, the Japanese Government does not worry too much about losing this investigative ability by allowing everybody to use strong encryption. "That leaves business interests in command of encryption policy inside Japan."[169]

Encryption's advantages, and not its potential dangers, seem to be what matters for shaping the future of cryptography in Japan. Japanese companies are focusing on providing privacy for electronic transactions, contemplating network payment facilities, and ensuring the identity of the parties in electronic transactions.[170]

Some Japanese officials suggest that cryptographic systems can all be broken. Therefore, the solution to law enforcement concerns is having good police decryption technology. In fact, the Japanese participation in the Organization for Economic Cooperation and Development's Meeting of Experts on Cryptography (which is reviewed below), showed little or no concern for national security issues.

Japan does not seem to separate digital signatures from encryption for privacy.[171]

[168] *See*: S. A. Baker, *Emerging Japanese Encryption Policy*. Available online at URL: http://www.us net/~steptoe/276915.htm.

[169] *Ibid.*

[170] *Ibid.*

[171] *Ibid.*

6. The Meeting of Experts on cryptography. Towards a global escrow system?

International cooperation will be critical in the future of strong encryption proliferation world wide. Many countries are worried about strong cryptographic products spreading into their borders. One of the international answers to these concerns was the Organization for Economic Cooperation and Development's Meeting of Experts on Cryptography held in Paris in December 1995 and co-sponsored by the International Chamber of Commerce [hereinafter ICC].[172]

This Meeting stressed that exchange of information on national encryption policies is one of the worldwide possibilities for future encryption regulation and it considered the creation of an international commercial key escrow system.[173]

Nevertheless, encryption export controls have been gradually labeled as "unworkable" by US software and hardware producers "who see a major market for security on the global information

[172] *See*: S. A. Baker, "*Summary of the OECD Meeting of Experts on Cryptography.*" Organization for Economic Cooperation and Development. Available online at: URL: http://www.us. net/~steptoe/276908.html. *See also*: D. Denning, *The Future of Cryptography.* Available online at URL http://www. eff.org/pub/Crypto/ITAR_export/Key_escrow/denning_ 02.

[173] *See*: S. A. Baker, *Ibid. See also*: (Anonymous) *Encryption: A Free Society's Dilemma*, *Supra*, note 83, at 16.

Recently, on July 30th., 1996, the "G7" group of nations met in Paris to discuss terrorism. Among several issues, the group recommended restrictions and controls on the Internet and the imposition of a key escrow or other system to allow governments to access personal encrypted mail. This meeting had a quick response from civil libertarians on the Internet. *See* : *Alert from a coalition of online civil liberties organizations.* August 7th., 1996. Available online at: URL http://www. aclu.org/gilc/index1.html.

infrastructure. This need, they argue, will be met by foreign producers if US export controls are kept in place".[174]

Perhaps one of the purposes of the OECD meeting of experts on cryptography was, for the USA, to show other countries that sooner or later they will have to favor a key escrow system to avoid problems that the criminal use of encryption may cause. From the US point of view, this was a chance to draw other Governments' attention to the chances they may be taking by neglecting encryption regulations or controls. Perhaps there was also the motivation of showing to the US crypto-industry that the fact that some encryption techniques have surpassed US Governments controls does not mean that the global market is open to non-escrowed encryption producers.

The US representatives tried to persuade the others that a local way of controlling encryption may be problematic. Some countries have expressed serious doubts about the US efforts in controlling encryption technologies. For instance, Japanese representatives showed little or no interest in controlling encryption. Other countries expressed their proclivity to favor some kind of escrow scheme (like France, the UK and the European Union), although there was almost a consensus on preferring to talk about Trusted Third Parties than about escrow agents on the key storage topic.

"Many European Governments are clearly interested in doing something to encourage key escrow encryption, and Australia and Canada are likely to follow, if a consensus in favor of key escrow emerges."[175]

There is, of course, the question of how well received the key escrow encryption system will be for international security solutions since it uses a US classified algorithm. At the experts meeting, the US representatives explained that the EES uses a classified

[174] *See*: S. A. Baker, *Ibid. See also*: (Anonymous) *Ibid.* at 16.

[175] *See:* S. A. Baker, *Ibid.*

algorithm, but they added that there is a plan of using a neutral algorithm.

At the end, it seemed like the concern of the USA was to provide a law enforcement access, whereas the European Community representation was more concerned about providing security solutions.[176]

The Canadian representation was not so enthusiastic about the Clipper proposal. Allowing the US government to hold a copy of the keys was not an acceptable idea for the Canadian Government. Canada did not expressly reject the idea of escrowing keys, but just the Clipper project becoming the international standard.

Among the participants on the Encryption Experts Meeting, the Australian representation had a suggestion which we believe very interesting and pertinent. They suggested that relying on court orders to require decryption was perhaps a more viable solution than requiring a review of the laws that deal with self incrimination.

The next OECD meeting will take place next February 9th., 1997, in Canberra. We can hope that it will end up with a workable plan that will clarify two crucial points: the future global perspective on encryption regulations and the future global trends of escrow systems.

International concerns for strong cryptography proliferation might soon end up with the creation of an international escrow system. This might be problematic since it would mean to review all domestic laws that deal with self incrimination. Therefore, it seems that the most seasonable proposal to solve this problem is to rely on court orders to force decryption and to establish an effective system of sanctions to discourage the criminal use of encryption.

[176] *Ibid.*

CHAPTER III. PRIVACY LAW ISSUES FOR ENCRYPTION AND GOVERNMENT CONTROL IN MEXICO.

1. Mexico on the threshold of the Information Highway.

A) Information technologies as a priority in the National Development Plan 1995-2000.

- *Mexico Online?*

B) The Informatic Development Program.

C) The Consultant Committee on Informatic Policies.

2. Privacy and communication security under Mexican Law. Overview of the various administrative and legal possibilities.

A) The Federal Public Administration Act.

B) The Federal Telecommunications Act.

C) The General Communications Channels Act.

D) Recent criminal law reforms.

i) The Criminal Code.

ii) The Federal Criminal Proceedings Code.

E) The Federal Act on Fire Arms and Explosives.

- Can encryption be a munition in Mexico?

-No: a Literal Interpretation Method..

- Yes: Interpretation of the constitutional basis of FAE and FAER.

3. Analysis of a hypothetical escrow system in Mexico. Constitutional considerations.

A) Constitutional Article 6: the Right to Free Expression of Ideas.

B) Constitutional Article 7: Freedom of Press.

C) Constitutional Articles 14 and 16: Guarantees of Legality and Justice.

D) Constitutional Article 20 II: Compelled speech.

E) Cryptography in Mexico: what analogy applies?

- i) Encryption as a personal paper, a possession, or document.
- ii) Encryption as a vehicle.
- iii) Encryption as a different language.
- iv) Encryption as a security measure.
- v) Encryption as an extension of the individual's domicile.
- vi) The ability to decide on the analogy.

CHAPTER III. PRIVACY LAW ISSUES FOR ENCRYPTION AND GOVERNMENT CONTROL IN MEXICO.

1. Mexico on the threshold of the Information Highway.

Around the world, advances in encryption technologies are increasingly ensuring the personal privacy of people who use it for communication or information storage. This makes it harder for Governments to intercept telephone lines, e-mail messages or other kinds of protected information electronically stored or sent. Encryption has a critical role to play in the data security development context. It will play a vital role not only for Mexico's social development, but also for its economic progress, by ensuring transactions and information regarding foreign trade and foreign investment.

Law is often slow and vague in responding to technological developments. In Mexico, the legal field dealing with security measures on information is almost completely barren. What will breach the gap in Mexican legislation? What constitutional issues may arise from this? With what legal response? Mexican law will face the imminent challenge of adjusting to new technological developments.

Interestingly, the OECD Meeting of Experts on Cryptography[177] emphasized the chance for escrow systems to

[177] *Ibid.*

become the global standard. This would certainly create several kinds of problems worldwide. In Mexico there would possibly be resistance to this system. In this chapter, we will discuss some of the most obvious impacts that an escrow system would have in Mexico. To do so, we first introduce the example of the US Escrow Encryption Standard project and then evaluate the hypothetical implementation of a similar escrow standard in Mexico.

This area is directly related to several issues that Mexico is already facing, for instance, telephone wiretapping. A few months ago, a telephone conversation of the Special Fiscal for the *Colosio* case was intercepted and made public in the Senate.[178] This case, however, is not isolated. It is publicly known, yet not legally permitted, that the Mexican Telephone service provider (*Teléfonos de México*) wiretaps telephone lines, complying with the "orders" it receives from the Ministry of the Interior.[179]

The need to regulate privacy in personal and commercial communications in Mexico was obvious even before the case mentioned above. However, the framework in which the country has to approach these issues is not clearly defined yet. In particular, "National Security" is a vague or disperse concept in Mexico. It is not defined yet in any body of law or jurisprudential thesis. Yet, it is increasingly becoming a main concern of law enforcement authorities. Even though it is not *per se*, it is indirectly approached via the *threats* to it, *i.e.* the combat to organized crime.

Recent changes to several constitutional articles and to the Criminal Legislation are a clear indication that Mexico wants to give strong bases to combat organized crime in a more effective way and through a specific legal framework. Some Congressmen have pointed out that "if in the future the Congress issues a law on

[178] *See: "PGR: Se Prepara una Iniciativa para Reglamentar el Espionaje Telefónico."* La Jornada, May 24th., 1995. Mexico City, Mexico. As a result, Mexico's Attorney General, Antonio Lozano Gracia, announced the Government's intention to regulate telephonic espionage

[179] *See: "Puentear líneas para Gobernación, orden de rutina en Telmex."* La Jornada, May 26th., 1995. Mexico City, Mexico.

national security, the executive -or any intelligence services- will be able to intervene in private communications, wielding State reasons."[180]

What steps is the Mexican Government taking in order to regulate these delicate questions?

At present, there are many proposals pending, almost all of which converge in two different approaches. First, there is an important criminal law reform being produced to enhance the combat against organized crime. Second, the Government is encouraging several administrative steps that will eventually help solve some difficulties on personal privacy.[181]

A) Information technologies as a priority in the National Development Plan 1995-2000.[182]

The global technological transformation opens new challenges and opportunities for Mexico. On May 8th, 1995, the Mexican Government published the National Development Plan for the period 1995-2000. The Plan mentioned some explicit guidelines that the public administration should follow in order to promote and increase the use of information technologies in the country. These

[180] *See*: *"Reunión de Procuradores y Ombudsman"*. La Jornada, April 29th., 1996. Mexico City, Mexico, at 8.

[181] Such a dichotomy, if not carefully handled, may create some difficulties. Law enforcement authorities will eventually, with legislation to combat organized crime, have more legal tools to meet their ends. An important challenge for this new law would be to achieve a balanced system by which both law enforcement abilities and personal privacy are ensured without interfering with each other.

[182] Office of the President of the United Mexican States. National Development Plan 1995-2000. May 8th., 1995. Available online at URL: http://www.inegi.gob.mx/homepara/pdi/

topics were always mentioned in close connection with important national objectives.[183]

In the field of Informatics[184], President Zedillo announced that the government will promote the formation of specialists at all levels and that the activity of the federal government will be focused on generating, spreading and applying all kinds of technological innovations. He emphasized the social implications of new information technologies and concluded that these technologies were strategic for the development of the country.

President Zedillo also said that new technological policies must begin with the diagnosis of today's situation in Mexico, and he recognized that the country was not using the great potential of new informatic technologies effectively. One of the main reasons for this is that Mexico has not followed any specific strategy to acquire and assimilate technologies available in other countries.

The delay in this issue provoked the Mexican Government to create the Informatic Development Program [hereinafter IDP]. The IDP is one of the 32 programs that the National Plan of Development 1995-2000 concluded will improve the quality of Mexicans' lives. This plan emerged as a result of Mexico's need for a strategy to make good use of information technologies.

[183] As was said, progress, control and better government are some of the values that can be achieved through the Informatic Development Program. These are vague concepts, but this study recognizes that "control" and "better government" can be in close connection with law enforcement. This is one of the essential parts of a future encryption policy, as examined later. *See*: *Infra*, Chapter IV, parts 1 and 2.

[184] This literal translation respects the original sense from the NDP Here, this concept is often used instead of "telematic", "technological revolution", "information technologies" or "technologic convergence in computational sciences, microelectronics and telecommunications to produce great volumes of information, check it and send it through enormous distances." *See*: National Development Plan 1995-200. *Supra*, note 182. Moreover, article 3-VII of the Statistic and Geographic Information Act (*"Ley de Información Estadística y Geográfica"*) published in the Federal Register on December 30th., 1980 defines "informatics" as the "technology for the rational and systematic treatment of information through electronic data processing." Thus, we will further use the term "informatics" to refer to all these different meanings.

Mexico online?

Mexico is among the 20 largest countries in the world, and yet it is ranked 33 by the International Telecommunications Union for telephonic density.[185] This illustrates that in order for Mexico to take real profit from the information highway some important problems will have to be solved, not only concerning quality of services, but also quantity.

Nonetheless, expectations for a growth of the services amount are very positive: INEGI estimates that telephonic density (per 100 habitants) in Mexico has grown from 11.5% in 1995 to 13.5% in 1996. The demand for *online* services has increased dramatically over the last few years (particularly Internet).[186]

B) The Informatic Development Program.

The Meeting to introduce the IDP 1995-2000 was conducted on April 12th., 1996. It recognized that electronic information has crucial advantages over written information (it is more practical, more manageable, and easier to store and recuperate). The Meeting also acknowledged that the role of information in the global context is critical for national economies, for people and industries. Thus, the Mexican Government has to develop an informatic infrastructure that provides a framework of confidence,[187] among other things.

[185] *See*: Graph no. 3, *infra*, at 154.

[186] *See*: Graph no. 5, *infra*, at 156.

[187] It is not completely sure whether this term refers on the IDP to build a systematic infrastructure that regulates and ensures confidentiality, privacy and authentication in similar terms to those referred to in this study since the IDP text is not so specific. Our advise to the Committee is to take into consideration the

The situation in Mexico is complicated, however. While the information revolution in the country is unavoidable and will affect all aspects of Mexicans' daily lives and culture in a very short term, only 2 % of the inhabitants and 3 % of the homes have a computer.[188] One of the main concerns of the Program is to promote the infrastructure in the country, allowing it to increase the growth of LAN. These Networks have became very important on both the international and the national levels of information exploitation. Network interconnection is now a requirement for administrating data electronically stored. The objective of the IDP is to promote an effective utilization of information technologies in the public, private and social sectors. One of the channels that the Meeting contemplated is the growth of online data networks and LAN, as well as the development of an appropriate regulatory framework for their use.

The Congress will work on these issues and will define the parameters to regulate, at least initially, important issues such as: intellectual property online, confidentiality and security on data processing and information flow systems, personal data protection on public and private networks and systems, security of public strategic information distributed through data networks, definition, prevention and punishment of online crimes, and definition of the value of electronic documents as evidence in criminal or civil procedures.

There are some projects already identified. Almost all of them aim to help authorities in law enforcement and justice. For instance, the National System of Public Security, which will be coordinated by the Ministry of the Interior, will support the activity of law enforcement authorities by creating criminal information data bases. Another example is the Data Bank of Crimes and Criminals.

Following the guidelines established by the National

proposals made here. *See*: *Infra*, Chapter IV, parts 1 and 2.

[188] *See*: Graphs 2 and 4, *infra*, at 153 and 155 respectively.

Development Program and working specifically on the IDP, the INEGI recently called a Forum on Informatics and the Law[189] (September 18th through October 18th, 1996.) The objectives of the Forum were to analyze, in five different meetings, the legal framework of the following:

1.- Individual's rights to confidentiality of information stored in public and private data bases, and the protection of strategic or confidential information.

2.- Computer crimes and computer records as evidence in judicial and administrative proceedings.

3.- Intellectual property rights for information transmitted via, or stored on, public data networks, as well as protection for software developers.

4.- Mechanisms to promote and develop the use of information technologies, and guarantee the fair competence between providers of computational services.

5.- Conditions for access to and exploitation of "telematic" services.

The first meeting brought interesting conclusions that are relevant to the topic of this study:[190]

a) There is a need to review international legislation on individual's rights to confidentiality of information, such as the

[189] *See*: "*Summon for the Forum on Informatics and the Law.*" August 9th., 1996. Congress of the United Mexican States. Available online at URL: http://www.inegi.gob.mx/homepara/pdi/.

[190] *See*: "*Relatoria del Primer Evento del Foro de Consulta sobre Derecho e Informática.*" Available at URL http://www.inegi.gob.mx/homepara/pdi/pdi/rela1. html. In this first meeting, one of the lecturers -Ing. Miguel Angel Alvarado S., President of the Latinoamerican Association of Professionals in Informatic Security- stressed that the non-existence of legislation that relates to electronic information, may provoke that public entities take in their own hands the right to control those data accordingly to their own interests, without owners consent.

French, the USA's, and other legislations that protect people's privacy.

b) It is important to educate people about the outcomes of informatic's misuse.

c) A crime online is not different from those crimes already typified.[191]

The third meeting brought one of the most important conclusions of the Forum: the need to adapt the Mexican constitution to today's needs on electronic data.[192] However, the meeting did not define the changes that such a modernization would imply. This modernization would necessarily have to define some issues that, unfortunately, none of the meetings mentioned (*e.g.* national security and individual's privacy), and set forth the principles to establish the system to balance them.

C) The Consultant Committee on Informatic Policies.

The IDP collected the opinion of experts, researchers, professionals, scholars, public servants and journalists, and analyzed all proposals. As a result, the Consultant Committee of Informatic Policies ("*Grupo Consultivo de Políticas Informáticas*" [hereinafter CCIP or "the Committee"] was created to advise the

[191] Contradictory, the second meeting concluded that it is necessary to typify online crimes, taking into account its own special characteristics. *See*: "*Relatoria del Segundo Evento del Foro de Consulta sobre Derecho e Informática.*" Available at URL http://www.inegi.gob.mx/homepara/pdi/pdi/rela2. html.

[192] *See*: "*Relatoria del Tercer Evento del Foro de Consulta sobre Derecho e Informática.*" Available at URL http://www.inegi.gob.mx/homepara/pdi/pdi/rela3. html.

National Institute of Statistics, Geography and [hereinafter INEGI][193] on the implementation of the IDP. It was also meant to assist the Congress in its tasks.[194]

The Committee elaborated a document called "Elements for Strategic Programs on Informatic Policies" in October 1994.[195] This document recognizes several important issues that are worth mentioning. First, in Mexico there is no system that responds to security needs. Second, the expectations for Mexico to offer products and services in a global scale are scarce. Third, for Mexico to fully make profit of the Information Highway's great advantages, it must soon regulate the confidentiality, security and privacy of messages and data.[196]

The legal possibilities on information technologies are very dispersed. The bodies of law that are examined here are the following: the Federal Public Administration Act, the Federal Telecommunications Act, the General Communications Channels Act, the Recent criminal law reforms to the Criminal Code and the Federal Criminal Proceedings Code, and the Federal Act of Fire Arms and Explosives.[197]

The administrative framework that relates to information technologies is as scattered as the legal one. There are several Secretariats (or Ministerial Departments) that have responsibilities in

[193] In Mexico the INEGI is the authority in charge of formulating national informatic policies. *See*: Statistic and Geographic Information Act, supra, note 184, at article 30-VII in connection with articles 33 and 34.

[194] Defined above, see *supra*, Chapter III, part 1, section B), 2nd. and 3rd. paras. The Congress will be assisted by the Consultant Committee on Informatic Policies, which depends on the INEGI.

[195] *See*: "*Elements for Strategic Programs on Informatic Policies.*" Consultant Committee on Informatic Policies. National Institute of Statistics, Geography and Informatics. Mexico. October, 1994, at 39. Available on-line at URL: http://inegi.gob.mx/homepara/pdi/

[196] *Ibid.*

[197] The Royalties Federal Act and the Intellectual Property Protection Act are out of the scope of this work since they relate to intellectual property rights. The Decree of Formation of the National Council of Science and Technology does not represent an interest for us here either, since it deals with Research promotion issues.

the field, such as the Ministry of Commerce and Industrial Promotion (in areas of foreign commerce and intellectual property), the Ministry of Public Education (in education, royalties, professions, and scientific and technological policy through its National Council of Science and Technology), the Ministry of Communications and Transportation (in telecommunications),and the Ministry of Foreign Affairs (in scientific and technological cooperation). Finally, as regards to security, the regulation of public and private data is the responsibility of the Ministry of the Interior.

This dispersion might appear natural because of the penetration of computers in almost every aspect of social life today. However, this situation dilutes the responsibilities that surround information technologies and makes it harder to design national strategies.

The Committee considered that, in general terms, there was a relatively stable framework to regulate Informatic activities.[198]

It appears that some legal modifications will be necessarily substantive because it is difficult to affirm that there exists any comprehensive legislation on the subject, given that its different aspects are regulated separately and contain many important gaps.[199] Some of these gaps require immediate attention. For instance, the use of information is an issue that has been mainly approached on the national agenda from the point of view of freedom of speech and mass communications media. The confidentiality of information, even though it has been dealt with in the debates, has not drawn the attention it deserves.[200] It seems that people identification is critical for fiscal, electoral, and public

[198] *See*: "*Elements for Strategic Programs on Informatic Policies.*" *Supra*, note 195.

[199] Luckily, the Forum recognized this dispersion and the need for this area to be reviewed. *See*: "*Relatoria del Segundo Evento...*" *Supra*, note 191. The third meeting of the Forum concluded, among other things, that there was a great need to promote the coherence on national legislation.

[200] *See*: *Infra*, Chapter III, part 2, section A), when we point out the two legal approaches to public security issues in Mexico.

safety purposes. At the same time, it is also fundamental to respect information privacy that will promote the effective use of information technologies (in every sphere the Government has mentioned for the NDP, be it public, social, private or governmental).

The whole title of the legal framework in the study elaborated by the Committee is vague and does not provide any concrete recommendation, neither on security measures to protect data or messages, nor on confidentiality.[201] It merely provides some vague guidelines for the years to come and concludes that the legal framework of telecommunications, royalties, and governmental acquisitions will have to be reviewed and eventually revised, at least partially, to protect individuals' rights in public communications networks. The almost complete de-regulation of protection technologies for telecommunications is one of the most important problems that Mexico faces today in this area, and one that may be problematic for the country's governance.

The Mexican Government will have different roles to play: a) as a coordinator of information policies, b) as the public infrastructure provider, c) as the promoter of national development, d) as a user of these new technologies, and e) as protector of individual freedom. The way in which the Mexican Government assumes these roles will be critical in the future utilization of information technologies in the country. This is a very interesting issue given the administrative dispersion in Mexico. How will the government manage to successfully perform all its functions? The Committee has proposed, adequately we think, the creation of an Inter-secretarial Commission on Informatics, a National Office for Policy, and other different Advisory Councils to help the Government with this task.[202]

[201] *See*: Elements for Strategic Programs on Informatic Policies. *Supra*, note 195.

[202] The IDP will be implemented by several organisms, besides the

2. Privacy and communication security under a Mexican Law lacunae. Overview of the various administrative and legal Mexican possibilities.

To date, information technologies in Mexico lack institutional and legal structure. The legal and administrative frameworks that relate, not only to information privacy protection, but also to information technologies in general, is very confused and dispersed. The absence of specific regulations that protect personal and commercial privacy is obviously dangerous. At best, public entities may assume the management of private information without the owner's consent, damaging his/her right to privacy. There is also the risk that other people (hackers) intervene and harm others' privacy. Thus, there is an imminent need for protection of personal and commercial data confidentiality in a coherent framework. Therefore, the work of the Committee should be mainly focused on defining a systematic solution to the present situation.

There are several bodies of law that refer to the area of

Consultant Committee of Informatic Policies, such as the Committee to Follow the Fulfillment of the IDP (which will combine the participation of the Ministries of the Interior, Public Accountancy, Commerce and Industrial Development, Administrative Inspection and Development, Communications and Transports, Social Development, Public Education, and Labor), the National Council of Science and Technology, the National Institute of Statistics, Geography and Informatics and Members of the Legislative and Judicial Powers. The other two organisms are the Federal Public Administration Committee of Authorities on Informatics and the Informatics Committee on State and Municipal Public Administration. *See*: IDP, *supra*, note 2, at s. 5.2.

information technologies, but it is yet difficult to find a systematization in treating this area. On the following section, we review these laws.

A) The Federal Public Administration Act.

National security[203] has an important facet, that of individual privacy protection. Encryption is a way to ensure individual, or commercial, or governmental privacy. However, as seen before, this can be construed as interfering with national security. The treatment of encryption in Mexico is not defined yet.

The two facets of public security are treated in a vague manner at the institutional level. On one hand, there is the law enforcement perspective which involves problematic topics, and possible limits, such as good morals, public peace and respect for others' private lives, whose protection is the responsibility of the Ministry of the Interior.[204] On the other hand, the technical perspective of information technologies in Mexico is slightly better defined as a responsibility of the Ministry of Communications and

[203] *See*: Federal Public Administration Act. (*"Ley Orgánica de la Administración Pública Federal."*) Published in the Federal Register (*"Diario Oficial de la Federación"*) on December 29th., 1976, at article 29-XVI establishing that the National Defense Ministry is the authority in charge of regulating fire arms carriage, commerce, transportation, storage, etc. Thus, if encryption is to deserve the treatment of being a weapon in the future (which we hope will not happen), it will be responsibility of the Defense Ministry to regulate its use and development.

[204] *Ibid.*, at article 27-XX, giving the Ministry of the Interior the abilities to preserve the respect to private life, public peace and public morals in communication ways such as radio and TV transmissions. Yet, the Ministry of the Interior does not have responsibilities to watch over private privacy respect.

Transports.[205]

Finally, the Ministry of Commerce and Industrial Development is in charge of regulating industrial property and transfer of technology,[206] as well as studying and establishing restrictions to importation and exportation of certain goods.[207] It is also responsible for promoting commerce and economic development. Secure international communication laws are important to that responsibility.

B) The Federal Telecommunications Act.

The new Federal Telecommunications Act,[208] raises some important points for the purposes of this study. It mentions, for the first time, the existing connection between telecommunications and security and sovereignty of the Nation.[209]

The Act defined what the terms telecommunications and

[205] This Ministry conducts programs and establishes the policies for the development of communications, according to the country's needs (*Ibid.* art. 36-II), promotes the technological development in this field (art. 36-I), and regulates the administration of federal services of electric and electronic communications and its linkage with other services such as telephone, telegraph, wireless communications, and remote data processing (art. 36-XXVI).

[206] *Ibid.* Art. 34-XII.

[207] The import of encryption products is not yet restricted, but if that was to be the case in the future, this situation would be the responsibility of the Ministry of Commerce.

[208] *See:* Federal Telecommunications Act, *supra,* note 16.

[209] *Ibid.*, art. 2.

private and public telecommunications networks mean[210] and stated that all telecommunications networks would be General Communications Channels, including them in the Federal Jurisdiction.

National Security, even though not specifically defined, was mentioned in this Act. Two examples are worth quoting. First, the Ministry of Telecommunications will make sure that some satellite space is reserved for national security networks.[211] Second, there is a provision granting the Government the power of requisition of the General Communication Channels, in case of war, natural disaster, or imminent danger to national security, peace or economy.[212] However, the significance of this term remains under the discretion of the executive and hence is uncertain. It seems that neither the courts nor the Congress want to approach this problem. Yet, it is unavoidable that at a certain point, but only in a national emergency, national security, which is increasingly used in Mexican legislation, will have to be defined.

The Act punishes the "interception of information transmitted through public telecommunications networks."[213]

In all, this Act seems to focus mainly on stimulating the development of telecommunications,[214] improving the quality and diversity of communications services, and reducing its cost, rather than comprehensibly regulating the telecommunications field.

[210] *Ibid.*, articles 3-XIV, 3-IX, and 3-X.

[211] *Ibid.*, art. 55.

[212] *Ibid.*, art. 66.

[213] *See: Ibid.*, art. 71, s. A, establishing the imposition of fines from 10,000 and up to 100,000 minimum daily salaries. The fine can double in case of recidivism.

[214] *Ibid.*, art. 7.

C) The General Communications Channels Act.

The General Communications Channels Act applies today to postal service routes[215] and telecommunications networks, only in those cases which are not covered by the specific legislation.[216]

This Act is the antecedent of the Federal Telecommunications Act. It also contemplates the requisition of the general communications channels in case of war or imminent threat to the peace or the economy of the country,[217] and forbids the interception of messages and news electrically transmitted that are not destined to the public domain.

All telecommunication regulations are now specifically provided by the Federal Telecommunications Act (see earlier comments[218]).

D) Recent criminal law reforms.

Constitutional articles 16, 20, 21, 22 and 73 have been under recent review as part of the intensified combat against organized crime. One bill[219] will eventually enable law enforcement authorities

[215] *See*: article 1-XI of the General Communications Channels Act (*"Ley de Vías Generales de Comunicación"*), published in the Federal Register on February 19th., 1940, and last modified by the Federal Telecommunications Act (*supra*, note 16).

[216] *See*: Federal Telecommunications Act. *Supra*, note 16, at art. 8.

[217] *See*: General Communications Channels Act, *supra*, note 215, at art. 112.

[218] *See*: *Supra*, Chapter III, part 2, section B).

[219] The Bill is called "*Proyecto de Ley contra la Delincuencia Organizada*", and it is being discussed in the Mexican Senate.

to intervene in private communications. Unfortunately, the bill did not draw any limits to this power, neither did it specify that private communications could *only* be wiretapped in the case of organized crime. Rather, it took the approach of excluding the cases in which interception would apply, *i.e.* the electoral, fiscal, labor, civil, administrative and commercial cases.

Mexico is about to enact a federal act to combat organized crime. The reach of this law is not clearly defined yet.[220] However, its constitutional basis is already set forth by the last reform to constitutional article 16, the Criminal Code, and the Criminal Proceedings Federal Code (described next). On September 3rd, 1993, article 16 of the Constitution was reformed to introduce the term "organized delinquency" to its text. The reason was two-fold. First, the reform referred to certain criminal organizations, with important economic power growth and great violence capacities, that did not fit into the simple term "criminal alliance" any more. Second, as a consequence of the first reason, the basic principle "*nullum crime sine lege*", made it difficult for the law to apply to these organizations.

This Mexican process of improving controls against organized crime, has not taken any measures to restrict the use or import of encryption products yet. Although there is an important concern regarding the issue of controlling organized crime and protecting national security, it would be sad for Mexico to adopt a regime as strict as the Russian or the French one, where personal and commercial privacy appear to be exposed to a high risk.

[220] The initial Bill has been attacked as a "flagrant violation to the [Mexican] Constitution" by the President of the Mexican Human Rights Commission. *See: "Aprobarla Sería Flagrante Violación a la Constitución"*. La Jornada. November 15th., 1995, Mexico City, Mexico.

i) The Criminal Code.

The Mexican Criminal Code[221] has also been recently modified. The reforms introduced important changes.[222] The key changes for the purposes of this study are, unfortunately, scarce. There are no specific parameters to regulate crimes *online* or deal with the protection of privacy on public networks or security of data electronically stored or sent.

Concerning the changes introduced by the reforms, the part referring to crimes against public health (drug-related crimes) is of some interest because it includes the confiscation of objects, instruments, vehicles and products of (or used to commit)[223] those crimes, expanding the abilities of the investigative authorities. Still, this is not enough if we think that drug dealers are often an economic force and, as such, they frequently have access to the highest technological innovations. A drug dealing transaction may involve different types of activities, most of which involve digital communications and data storage. So, the question here is if at a certain point a drug-related criminal uses encryption for the purposes of drug trafficking , will courts be entitled to force him/her to disclose encrypted information? Also, what will happen if the criminal used encryption techniques to sell or buy the drugs? Will the courts then say that encryption techniques were the means or "vehicle" for committing the crime? What would happen with all the encrypted evidence needed to convict him/her? How are courts going to force decryption of this evidence? These are the kind of

[221] Criminal Code for Mexico City in Common Jurisdiction, and for the entire Republic in Federal Jurisdiction ("*Código Penal Para el Distrito Federal en Materia del Fuero Común y para toda la República en Materia del Fuero Federal*"), published in the Federal Register ("*Diario Oficial de la Federación*"), August 14th., 1931, Mexico.

[222] *See*: Plascencia Villanueva, Raúl. "*La Reforma al Código Penal Para el Distrito Federal en Materia del Fuero Común y para toda la República en Materia del Fuero Federal.*" Available on-line URL http://info.juridicas.unam. mx:80/infojus/

[223] This term is broad and leaves the door open for the discretion of authorities to include information technology as "equipment to further the crime".

unsolved issues that, sooner or later, will become problems for courts. To date there is no certain basis on which to decide how courts will deal with them. Unfortunately, these latest criminal reforms are of no help in solving these issues.[224]

The general conclusion is that legislators were not concerned with information technology in the Mexican Criminal Code Amendments reviewed here.

ii) The Criminal Proceedings Federal Code.

The Federal Code of Criminal Procedures also received important changes.

This Code established the definition of the term "organized delinquency" as the "organization in which intervene three or more people, under certain hierarchical and disciplinary rules, to repeatedly, or in a violent way, or with remunerative ends, commit some of the crimes described in the following articles..."[225] The articles that follow mention these crimes: terrorism, sabotage, piracy, prisoner escape, attack on federal channels of communication, unlawful utilization of air transit installations, crimes against public health (drug-related crimes), rape, hijacking, murder, kidnapping, some cases of aggravated theft, bribery, and some cases of arms traffic.

As we can see, the concept of organized delinquency does

[224] We have a proposal to solve some of these issues. *See*: "Legislative proposal on lawful decryption", *infra*, Chapter IV, part 2.

[225] *See*: Article 194 bis of the Federal Code of Criminal Procedures *("Código Federal de Procedimientos Penales")*. Published in the Federal Register *("Diario Oficial de la Federación")*, November 17th., 1931. Mexico,

not refer to an autonomous criminal type, but as an aggravating circumstance of some crimes, since "organized delinquency" is not a crime in and of itself, as it occurs with a criminal alliance or gang. It seems that the Mexican approach is distinct from other countries' perspectives on "organized crime", where the continuance of the organization is one of the main characteristics. This feature, however, is not comprehended on the description we mentioned of "organized delinquency".

Again, one can conclude that information technologies were not on the legislators' minds for these amendments.

E) The Federal Act on Fire Arms and Explosives.

Above, we discussed the international efforts that are being carried out with regard to encryption.[226] Internationally, there are several examples that treat encryption products as a munition.[227]

An important area of concern in technological advances on encryption is related to cellular phones. In Europe, there is a cryptographic algorithm called A5 that is used to encrypt a cellular phone system: the Global System Mobile [hereinafter GSM]. This system is considered a non-exportable munition and is thus classified. "In fact, NATO has used its powers to limit GSM export under its COCOM agreement. This has prompted GSM companies to create A5X, a weaker version of A5 that is easier to crack and exportable."[228]

[226] *See*: *supra*, Chapter II, part 6.

[227] *See*: ITAR, *supra*, note 98; France's *Loi sur les Telecommunications*, *supra*, note 156; and South Africa, *in:* J. P. Chandler. *Supra*, note 65.

[228] *See*: *supra*, (Anonymous) *Encryption: A Free Society's Dilemma*, *Supra*,

In this section, we discuss the challenge for Mexican legislation in trying to define the status of encryption products.[229] Will Mexico categorize strong encryption systems as munitions? If so, on what bases? Would the reasons why the State regulates firearms and explosives be the same as those used to regulate encryption technologies?

Several arguments could be given to support either a yes or a no answer to the question of status of munition. It is worth analyzing both perspectives.

No: A literal interpretation method.

Under the present legislative terms, the Federal Act of Fire Arms and Explosives [hereinafter FAE][230] and its Regulations [hereinafter FAER][231] are literally restricted to fire arms. These bodies of law do not leave a door open to allow the term "fire arm" to refer to a strong encryption product. The language used in the Act and its Regulations is simple and straightforward: both talk about pistols, revolvers, shot guns, rifles, machine guns, fusels, carbines, cartridges, canons, artillery equipment, mortars, projectiles, torpedoes, grenades, bombs, mines, flame throwers, bayonets, sabers, lances, war vessels, submarines, missiles,

note 83, at 17. *See also*: S. Levy, *"The NSA is Not Alone"*, Wired 1. February, 1993. Available online at URL: http://www.hotwired.com/wired/1.2/features/crypto.rebels.sidebars.htm#nsa-not-alone.

[229] The reason why encryption technologies are treated as munitions in other countries is that they are "potential dangers" that can allow terrorists and other criminals to escape the reach of the law if they further their crimes using these technologies. This will eventually make impossible for the authorities to know about criminals' activities and even gain access to the evidence that could lead to their conviction.

[230] *See*: Federal Act of Fire Arms and Explosives (*"Ley Federal de Armas de Fuego y Explosivos"*), published in the Federal Register (*"Diario Oficial de la Federación"*) on Jan. 11th., 1972, and last amended by Decrees of July 22nd., 1994 and December 21st., 1995;

[231] Federal Act of Fire Arms and Explosives' Regulations (*"Reglamento de la Ley Federal de Armas de Fuego y Explosivos"*), published in the Federal Register (*"Diario Oficial de la Federación"*) on May 6th., 1972.

munitions of other types, gases and chemical substances of exclusively military usage.[232] Besides, article 41 of FAE restricts the application of several substantive dispositions to arms, munitions, explosives and chemical products and substances used in connection with explosives.

Thus, it seems like the present terms of FAE and FAER do not provide the opportunity of including cryptography as another munition.

However, it might be not so critical whether or not the vocabulary of those two bodies of law may include encryption. The problem could be solved if, by Decree, the Mexican Congress reformed the Act and its Regulations by adopting a system that included cryptographic methods as another munition in the listing. This would not be an easy solution at all, though, because reforming these two bodies of law would obviously require an exhaustive review of Mexican legislation that relates to the area. What appears more important is try to decide whether or not it is worth treating strong cryptography as munitions.

To answer the question, we have to determine two things: first, what reasons may a State have to regulate firearms and explosives; second, what reasons may a country have to restrict encryption. Once identified, these reasons must be analyzed to decide whether they are sufficient to restrict encryption utilization without conflicting with constitutional rights. For instance, one of the US Government's most important arguments to regulate encryption products export is national security protection. Nevertheless, to date national security is not sufficient to limit domestic use of encryption too.

Mexico does not have to worry about limiting the export of any encryption product today, but the domestic use of encryption is a separate question. So, we may wonder what arguments could give

[232] *See*: Federal Act of Fire Arms and Explosives, *supra*, note 230 at articles 10 through 12 making this enumeration.

support to restrict the use of encryption in Mexico. Could Mexico introduce a national security argument to limit domestic utilization of encryption?[233] What does this term mean in Mexico and is it justifiable, then, to include encryption as a munition in Mexican legislation?

Both FAE and FAER are meant to regulate the private use of arms, by restricting the use of military-grade munitions to the Mexican Army. There are several articles that include a detailed description of which kinds of arms are strictly meant for military use,[234] and there are also specific punishments for civilians who possess, carry or use those weapons.[235]

Therefore, the main questions remain unsolved with a strictly literal interpretation method.

Yes: Interpretation of the constitutional basis of FAE and FAER.

A study of the constitutional source for FAE and FAER, *i.e.* constitutional article 10, is helpful since it determines the reasons why the State regulates firearms and explosives.

This article states that Mexicans have the right to possess

[233] In Mexico, national security is not clearly delimited, and is mostly construed as a national emergency provoked by an attack to the State's sovereignity. This has not occurred for a long time since even the Chiapas conflict was not perceived by the Mexican Government as a national security threat. Mexico does not have a bellicose background as extensive as the USA. Thus, terrorism and bombing (the main worries of national security protection in the USA) do not represent an actual threat in Mexico.

The State's reason to regulate firearms and explosives in FAE and FAER is two-fold: to restrict the use of certain military-grade arms and to provide an adequate legal framework that allows citizens to possess arms for protecting and securing their personal and familiar privacy. From this perspective, the Mexican system of enabling personal privacy protection potentially favors the use of encryption technologies for this end.

[234] *See*: articles 7 through 12 of the Federal Act of Fire Arms and Explosives *supra*, note 230.

[235] *See*: *Ibid*. Articles 77 through 91.

arms in their domiciles for their security and lawful defense, with the exception of those arms restricted to the Army.[236] The exposition of the aims of this article state several points worth mentioning.[237] First, it was the imminent need for regulating people's arms possession for their *security* and lawful defense that motivated the creation of this personal right. Second, the juridical quality that this article protects is precisely *personal security*. Third, the regulation of this issue is also needed to protect the collectivities from "unlawful munitions carrying". Fourth, carrying or possession of arms should not imply a danger in itself for the collectivity.

Today, arms carriage has the following limitations. First, arms can only be carried with a specific license. Second, only permitted arms, as opposed to military-grade arms only allowed to the Army, can be subject to private possession and carriage. Finally, the object of private arms possession must be to protect one's security and lawful defense.

So, from those premises, and if we accept that encryption is a *personal security measure* some ideas may be inferred to determine whether strong encryption methods can be considered arms. If we take into account the reasons behind constitutional article 10 and make a comparative analysis of them with respect to encryption, it can be inferred that most of them may apply to encryption. Encryption technological systems would be a lawful munition if they complied with two characteristics. First, they should be used to protect one's personal security. Second, they should imply no danger in itself for the collectivity. Obviously, encryption software or hardware are not inherently harmful.[238] Encryption can not be considered as a danger in itself, even when used on crime furthering, since the criminal act and the medium for committing it

[236] Political Constitution of the Mexican United States, (*Constitución Política de los Estados Unidos Mexicanos*), Published on February 5th., 1917. Editorial Porrúa. Mexico, 1992, at article 10.

[237] *See*: I. Burgoa Orihuela. *Las Garantías Individuales*. Editorial Porrúa. 26th., edition. Mexico, 1994, at 396.

[238] Except when included in a computer virus program.

are different.[239]

As regard requirements for arms carriage or possession that were described above, there is one limitation that would represent a problem to encryption as a munition. The Mexican system distinguishes between military-grade arms and common-use arms. So, the question would be to differentiate between *strong* or military-grade encryption programs and common-grade programs in Mexico. At first glance, this question would not be so difficult to answer because the treatment of encryption products in Mexico would probably be based on the international treatment that a certain product receives abroad,[240] but any decision would need to be more specifically based and justified at the national and international levels. Besides, another important question that would have to be addressed before deciding to establish the system is whether it would be useful to make such a differentiation.[241]

Just as the questions outlined above, many controversial legal points will surely arise in Mexico. The work done by the Committee will be critical for the future of communications online in Mexico. The Consultant Committee on Informatic Policies should try to analyze and foresee the possible impact of encryption use in Mexico in the conflicting areas of personal vs. national security, and it should benefit from other countries' experiences on the issue.

[239] An important argument against these ideas, however, is that Mexico lacks the elements of a bellicose background and terrorist attacks that in other countries have motivated the treatment of encryption as a munition.

[240] The question is not so easy to answer, though, because the same algorithm often receives different levels of restriction internationally. *See*, for instance, the inconsistent international treatment that DES receives (*supra*, Chapter II, part 3, when we refer to DES.)

[241] It would not be so convenient to make this differentiation because first, this is internationally proven to be almost fruitless (since many strong cryptographic products are freely available on the Internet) and second, it would require the establishment of a whole control system for domestic use and importation of these products.

3. Analysis of a hypothetical escrow system in Mexico: Constitutional considerations.

Even though Mexico has not yet published any specific regulation concerning encryption[242] it is imminent. At some point it will have to set, at least, the basic parameters to regulate this important issue because one thing is for sure: information security concerns will grow as foreign trade and foreign investments increase in the country, and the framework built will determine many critical issues.[243]

It was said earlier[244] that the future of military-grade encryption worldwide will depend in an important way on international cooperation to regulate it (or perhaps de-regulate it). The different approaches that the OECD Meeting[245] put into perspective were also emphasized.

In this section, we try to speculate on the implementation of an escrow system in Mexico and attempt a constitutional analysis. For Mexico to adopt such a standard would require the import of

[242] To date, article 52 of the Mexican Foreign Service Act's Rules (*Supra*, note 40) is the only one to mention encryption in the whole Mexican legislation. It only refers to the means for protecting diplomatic "document's confidentiality... and other communication systems". There is no general jurisdiction determined over cryptographic systems yet because, even though this provision is meant to be a responsibility of the Foreign Affairs Minister (*"Secretaría de Relaciones Exteriores"*), it is specifically limited to be in connection with diplomatic and consulate services.

[243] It is worth mentioning that Mexico presents an almost complete lack on encryption treatment, from literature to legislation.

[244] *See*: S. Baker, OECD Meeting of Experts on Cryptography, *supra*, note 172.

[245] *Ibid*. *See also*: Dorothy Denning, *The Future of Cryptography*. *supra*, note 172.

the technology since to date there is no domestic production of cryptographic devices. Our comparative framework is therefore based on a system like the USA's EES.[246]

Therefore, we will suppose that the adopted Mexican encryption system would consist of a key escrow method and that, as a result, the Government would propose to split the chips' keys in two and give each part to a different escrow agent keeping the family key for itself. Such a body of law would probably conflict with some of the Basic Rights ("*Garantías Individuales*") established in the Political Constitution of the United Mexican States ("*Constitución Política de los Estados Unidos Mexicanos*") with respect to concepts such as a) the right of information (article 6), b) the prohibition against establishing any kind of "previous censure" to the freedom of speech or of press (art. 7); c) the guarantee of lawful security for the people not to be deprived of their liberty, papers and property without the completion of a judgment that lawfully concludes and orders it (art 14); d) the guarantee of justice that prohibits the public powers to search any body's person, domicile, papers, possessions, etc. without the proper warrant (art. 16); and e) the compulsory production of decryption keys from criminal defendants as an issue of compelled speech (art. 20-II).

[246] We will not get into detail of the transactions between the two Governments, US and Mexico, in order for Mexico to obtain access to EES technology; neither which of the systems (discussed above, Chapter II, part 3, when we make some comments on EES) would the two Governments adopt about the family keys. We will focus on the main constitutional issues that would arise since the adoption of an escrow system. We follow the example of the EES because it is more widely explored and represents one of the leading proposals in the field, even might not be the most suitable one.

We must stress that EES is useful for us only to the extent that it does not relate to export controls. We do not deal with EES from the point of view of replacing any exportable system in Mexico, obviously, but from the point of view of its mere implementation in Mexico.

A) Constitutional Article 6: the right to free expression of ideas.

The Mexican Constitution states: "Free expression of ideas shall not be the object of any judicial or administrative inquisition, but in the cases of attacking good morals or the rights of third parties, or when it constitutes a delict or public order disturbance; the State shall guarantee the right to information".[247] The free expression of ideas, as a derivation of freedom in general, represents one of the essential components of social and cultural development. The Constitution establishes this right with two components: the personal freedom to manifest ideas without any other restrictions than those mentioned by the Constitution itself, and the obligation for the State to guarantee the right of information. Unfortunately, the Constitution does not specify the way in which the State will comply with its obligation of watching over the right of information. The limits of this term are fuzzy and should always be carefully defined. The reason is that the State's will to grant accurate information may turn into a violation of the freedom of expression of ideas.

"The freedom of thought is completely linked to the freedom of expression on its most broader sense, *i.e.*, using all means of communication, from oral and written expression to the most developed and technical ways of communication and broadcasting..."[248] In this way, one should not confuse construing article 6 as addressing press freedom, protected specifically in article 7. Thus, we can conclude that article 6 protects the freedom of expressing ideas (opinions, thoughts, etc.) through speech, as well as other means, be they written (like art expressions in all of its

[247] Article 6 of the Political Constitution of the United Mexican States. *See: Supra*, note 236.

[248] *See*: I. Burgoa Orihuela. *Supra*, note 237, at 349, quoting Professor Sigfrido Obregoso, *Revista de Derecho y Ciencias Políticas y Sociales*. Year IV, No. 11, November 1968, at 243-244.

forms) or in any other form (like television, radio or cinematography).

As regards to the limitations on this right, it is unfortunate that the Supreme Court has not defined what the terms "morals", "rights of a third party" and "public order disturb" mean. This makes such limitations dangerous to the right of expression of ideas, and even useless[249] because first, attacks to public morals are typified by the Criminal Code,[250] as well as any other delict perpetration. Second, it is precisely the commission of a delict which would disturb the public order or attack the rights of a third party. So, it would be enough for this constitutional principle to state that the only limitation to the freedom of expression of ideas is the commission of a delict.

Based on the scheme described in article 6, a mandatory key escrow system would probably encounter a serious barrier here.

If one person wanted to communicate with another through electronic means, and wanted this communication to be private, but wanted to use other encryption methods than mandatory escrow, an interesting conflict would then arise. We must keep in mind that this communication is protected by article 6 and that its only real limit is the commission of a delict.[251] Thus, in order to impose the mandatory escrow scheme, the Government would need to typify as a crime the use of any encryption means different from escrow. Under this line of reasoning, mandatory escrow would violate article 6, among others, since it would equal to restrain the means for expressing ideas.

[249] *See*: I. Burgoa Orihuela. *Ibid.* at 353.

[250] *See*: Criminal Code, at articles 200 through 209. *Supra*, note 221.

[251] We have discussed why we think that the other limits to this right converge in delict perpetration. However, it must be stressed that the words "public order disturb" have been used before as a tool to attack the free expression of ideas. *See*, for instance, the reform of October 30th., 1941, to the Criminal Code (published in the Official Register on November 14th., 1941). This reform introduced the "crimes of social dissolution" in article 145, which equaled a direct (yet completely "constitutional") restriction to the freedom of speech by arguing "public order disturb". *See also:* the comment of Professor Burgoa on this topic, *supra*, note 237, at 353.

B) Constitutional Article 7: Freedom of Press.

Article 7 establishes the "inviolable freedom of writing and publishing writings over any subject. No law or authority shall establish the previous censure... or any restriction to the press freedom, which has no other limits than the respect to the private life, to the good morals and the public peace..."

As seen above, the freedom of press is protected by the Mexican Constitution with the only restrictions of respecting private life, good morals and public peace.[252] On the individual rights regime established by the Constitution, the essence of these civil rights has been interpreted as freedom, in both of its forms: freedom of thinking and freedom of acting. Freedom of acting can lead to all manifestations of human activity as long as it does not threatens the social order stability, the institutions, the public peace and other people's rights.[253]

Thus, the implementation of an EES scheme could face some

[252] These restrictions are, again, quite vague and inexact. The term "private life" can be construed almost as any act. The Supreme Court has not resolved this question. It has only established the distinction between the public and the private life of a public servant, the public life consisting of those acts that the individual fulfills in his/her performance as a public servant. (*See: Semanario Judicial de la Federación.* T. XXVI, epoch 5, at 975.) The other restriction, *i.e.* previous censure, refers to the assessment concerning the "convenience or inconvenience" of a certain printing before its public distribution, which is forbidden by article 7. To determine what activities may be construed as attempting to other's "private life", as well as determining what exactly the terms "attacks to public morals or public peace" mean, the criterion of delict perpetration appears to be the most convenient one.

[253] *See: Semanario Judicial de la Federación,. Amparo penal en revisión* 11290/32, February 8th., 1934, unanimity of 5 votes. Reg. 215, year 1934, epoch 5, t. XL, at 1275. *See also: Ibid. Amparo penal en revisión,* February 8th., 1918, majority of 6 votes. Reg. 221, year 1918, epoch 5, t. II, at 395.

difficulties in this direction, such as the following. First, since key escrow legislation would apply to communications, regardless of its content it could be construed (properly or improperly) in a sense that would restrain the freedom of speech. Secondly, even though encryption can enhance communicative privacy by contemplating anonymity as a feature, the EES includes a critical degree of identification of the subjects, which can yield objections as to the threat to anonymity of both parties on a communication. Finally, it could be argued that EES complicates the associational freedom of people who want to gather but do not want to call attention about their association or their participation in it. We believe, nonetheless, that none of the above mentioned arguments concerning article 7 would find grounds enough to stop EES implementation.

C) Constitutional Articles 14 and 16: Guarantees of Legality and Justice.

Article 14 guarantees that "nobody can be deprived of his/her life, liberty, possessions or rights, but by virtue of judgment followed by the Court previously established to this purpose, and which complies with the essential formalities of the respective legal procedure, and accordingly to the laws enacted in advance to the fact."[254]

"Possessions"[255] can be construed to the extent of

[254] The essential formalities of the proceedings referred to in Article 14 have been defined as the opportunity given to the complaining party to be heard on the criminal proceedings drawn up against him/her and supply the evidence that might be suitable to his or her interests. *See*: *Ibid. Amparo directo* 539/92. Reg. 8426, year 1993, epoch 8. January, 1993. Unanimity of votes.

[255] The possession protected by either article 14 and 16 is *de facto*, *i.e.*, is strictly material and independent of both, the cause that originated the possession itself, and the right of possession. Thus, it is not relevant at all neither the way in which the person acquired the goods, nor the origin of such

representing personal data and information. The article states that no one can be "deprived" of his/her possessions; this term has been construed by the Supreme Court to apply not only to a confiscation, but also to any dispossession.[256] Therefore, under the present-day terms, the key escrow system would, thus, find a very important obstacle here: whenever the Government would need to decrypt data it should, first, complete the lawsuit (and succeed in it). Then, it should obtain a warrant or authorization from the judge to ask the escrow agents to provide their parts of the chip key and join them to finally disclose the contents of the message, following the procedures we have described above.

The main problem we see with this situation is that the encrypted data will often embody information that is important for the Government to access quickly, and to conclude a trial before getting access to these data, represents a substantial delay.

There would be a "shorter" way for the investigative authority, however: a written warrant from the competent authority (*i.e.* judiciary), given under the terms of article 16 of the constitution.

This article states that someone's person, family, domicile, papers or possessions, can not be searched unless "by virtue of a writ issued by the competent authority that founds and justifies the legal cause of the proceedings."[257]

possession. *See: Ibid.* Reg. 4146, year 1988, epoch 8. *See also: Ibid. Revisión principal* no. 425/87, reg. 6348, year 88, epoch 8. September 29th., 1988. Unanimity of votes. *See also: Ibid.* November 4th., 1918. Unanimity of 8 votes. Reg. 638, year 1918, epoch 5, t. III, at 1163. *See also: Ibid. Amparo Civil en Revisión* 402/40. Unanimity of 4 votes. July 24th., 1941. Reg. 905, year 1941, epoch 5, t. LXIX, at 1329.

[256] The deprivation must be definitive, and not temporary. *See: Ibid.* June 6th., 1919. Unanimity of 11 votes. Reg. 635, year 1919, epoch 5, t. IV, at 1119.

[257] Article 16 of the Political Constitution of the United Mexican States, *supra*, note 236.

Article 14 does not govern the rules for the writ referred upon in article 16, says Mexican Jurisprudence on the subject, because there is no reason to believe that the 1917 Constitutional Congress would have included under the general preventions of Article 14 those special acts that it chose to regulate under the terms of Articles 16 and 19. Thus, it would be nonsensical to believe that Article 14 protects the freedom of the individuals in such a broad sense that it allows violation of the writ of Article 16. [258]

As regards to the freedom of the individual, there is a criterion that establishes that personal liberty can be legally restricted by virtue of criminal responsibility because the former is always subordinated to the latter.[259]

As for the motivation requirement is concerned, this is not fulfilled if the authority only mentions the body of law as the foundation of its acts. It must make a citation of the specific precepts on which it bases its act.[260] This means that the judicial authority is compelled to base the *cause* of the proceedings as a whole and not to each and every assessment of the writ separately.[261] Moreover, a judicial determination is only motivated and based properly when directed to the person that the resolution itself is going to affect.[262]

[258] *See: Semanario Judicial de la Federación, Amparo penal en revisión* 3941/37. Reg.. 620 & 895, Year: 1937, Epoch: 5, T. LIII, p. 2568. September 3rd., 1937, unanimity of 5 votes. ***See also: Ibid. Amparo en revisión*** 212/90. Reg. 5736, year 91, epoch 8. June 28th., 1990. Unanimity of votes.

[259] ***See: Ibid. Amparo Penal en revisión.*** Reg. 407, year 1920, epoch 5, t. vii, at 1120. Majority of votes. The term "personal freedom" has been defined as "the right that every human being has by virtue of his/her own nature, and that the law does not know, but recognizes it; but if, for the circumstances provided by the law, the individual is deprived of his/her liberty, then it emerges the right for him/her to be free again, but by accomplishing certain requirements." ***See: Ibid.*** Reg. 7451, year 1923, epoch 5.

[260] ***See: Ibid. Amparo en revisión*** 7005/65. Reg. 844, year 1968, epoch 6, vol. CXXVIII, 3rd. part, p. 54. ***See also: Ibid. Amparo en revisión*** 5097/58, January 30th., 1961, majority of 3 votes. Reg. 770, year 1961, epoch 6, Vol. XLIII, 3rd. part, at 14.

[261] ***See: Ibid. Amparo en revisión*** 508/89. July 4th., 1991. Unanimity of votes. Reg. 5815, year 91, epoch 8.

[262] ***See: Ibid.*** February 29th., 1929. T. XXV, Reg. 904, year 1929, epoch 5.

Article 16 also enacts the requirements that every search warrant[263] must comply with: a) being issued by the competent[264] authority (judicial); b) being written; c) expressing the place to be inspected, the person or people to be apprehended, and the objects to find, limiting the proceedings to these parameters; d) drawing up a certificate of the proceedings completed, describing all its circumstances, in the presence of two witnesses.[265]

Administrative searches[266] *("visitas domiciliarias")* in someone's domicile are allowed, but they are limited to make sure that sanitary and police rulings are being observed or to demand the exhibition of tax-related documents. The same requirements and formalities that apply to the search warrants are applicable to administrative searches.[267]

Unanimity of 5 votes.

[263] Seizure writs are expressly authorized by the Constitution itself, whenever the requirements for search warrants enacted by Article 16 are observed. This warrant is, however, different from the seizure warrant established in Article 14 because the latter is due to the imposition of a criminal punishment. *See: Ibid. Amparo en revisión* 59/91. Reg. 3769, year: 91, epoch: 8. April 30th., 1991, unanimity of votes.

[264] The term "competence" has been interpreted by Mexican Courts as follows: the competence itself does not constitute a guarantee for the individual that the authority has been appointed accordingly to the proper law. Thus, if they were vices on the authority's appointment, and it committed an act against the citizen's interests, this would not directly imply a violation of the individual's fundamental rights, nor it would mean that the authority's proceedings are illegal or invalid. *See: Ibid. Amparo administrativo en revisión* 5377/44, April 20th., 1945, unanimity of 4 votes. Reg. 589, year 1945, epoch 5. T. LXXXIV, p. 910.

[265] *See:* Article 16 of the Political Constitution of the United Mexican States, *supra*, note 236.

[266] Even though the Government could find a valid argument as to the legitimacy of searches and argue that the cost for personal privacy would be low, people would hardly accept key escrow.

[267] According to article 16 first paragraph of the Constitution (*supra*, note 236), the individual is protected against arbitrary acts of annoyance on his/her person, family, papers or possessions. The rest of the sentence of this principle refers to the conditions under which authorities can utter valid acts of annoyance. Farther on, the same article sets forth the parameters for administrative searches in order to make sure that the citizen has complied with certain sanitary and police rulings and to demand that the individual to produce tax papers and accounting books in order to verify that he or she has observed tax regulations. In these cases, the authority shall follow the same guidelines and formalities prescribed for search warrants. Interpreted backwards, this article

However, the Government's right to searches does not empower it to demand the participation of the people to *create the conditions* that make searches effective.

We must bear in mind that the key is the means to decrypt a communication or data in order to uncover its content and, therefore, the disclosure of a key might resemble the disclosure of a private paper since both documents have the content of personal information. Thus, citizens are protected by article 16[268] against mandatory EES even when the Government would have the right to search someone's possessions or papers.

To sum up, the Government's right for searching would certainly not mean that one should furnish all the necessary items (in this case the chips key or the session key of a communication) to make the search effective.

Would the mandatory key escrow of the chip's key constitute a "search" under the terms of article 16 and a "seizure" under the terms of article 14?[269]

Even though the provisional measures that the investigative judiciary authority dictates in criminal investigation proceedings in order to seize the goods of the "indicted" are "acts of annoyance",

establishes some benefits for the citizen as regards to administrative searches, such as the protection of the domicile and documentation. This provision is not meant to limit the authorities' means of verification to administrative searches only. *See*: *Semanario Judicial de la Federación*. Reg. 6814, year 90, epoch 8, *Amparo en revisión* 250/39. March 30th., 1990. Unanimity of votes.

[268] Article 16 has been determined to be inapplicable to foreigners. *See*: *Semanario Judicial de la Federación*, Reg. 2450, year 1924, epoch 5, t. XIV, p. 286, January 17th., 1924, unanimity of 8 votes.

[269] The juridical goods protected by the guarantee of security are: life, property, possession and rights of the individual. It is precisely through the concept of *rights* that this guarantee reaches an important protective benefit to the people because it comprehends *any* right. The Mexican Supreme Court of Justice has defined the extent of the guarantee of audience, stating that it protects all the rights of the individual. *See*: *Ibid*. T. LVII, at 588.) "In order to the audience to be correct and real, the authority must not only hear the citizens and receive their evidences, but also to provide them with the necessary elements that allow them to properly structure their defense." (*Ibid*. 7th. epoch, t. XX at 6867).

like those mentioned in article 14, they do not violate the audience right established in the same article. The reason is, a court thesis says, that "since they are temporary, and thus do not mean a definitive deprivation of rights... they do not require to accomplish the requirements for deprivation acts established in article 14."[270]

In our case, however, construing the right of audience, as established in the above mentioned thesis, only to the limit of protecting "non-definitive" deprivations of rights would be especially dangerous and problematic. Why? Because only certain actions could be considered as definitive and since no investigative authorities can impose definitive acts, it would signify to give this investigative authority (inferior to the jurisdictional one) the right to demand disclosure of content of encrypted data whenever somebody is, *presumably*, doing something considered illegal.

Another thesis sets forth that the audience right (which is previous to the emission of an authority act), along with the due legal process, are both compulsory "only in case of deprivation acts referred to the life, freedom, property, possessions or rights of the individual, but not in case of deprivation of some of his/her goods or rights, because such acts are solely governed by the guarantee of juridical security (fundamentation and justification) established by article 16."[271]

The search is a Governmental invasion of the personal privacy of citizens. Yet, not all Government's access to information of individuals are necessarily a search, for instance, when dogs in the airports sniff someone's luggage or when someone is arrested and consequently searched. The cryptographic system's goal is to achieve or increase privacy, either in single-key or in public key

[270] *See*: *Ibid.* Reg. 8127, year 1993, epoch 8. Thesis no. X/93, January 12th., 1993.

[271] *See*: *Ibid.* Reg. 489, year 1975, epoch 0, Vol. 81, 3rd. part, p. 15, *Amparo en revisión* 1389/71. September 4th., 1975, 5 votes.] From our point of view, this thesis contains an important contradiction: how could we distinguish between "property" or "possessions" and "goods"? The problem has not yet been solved by the Supreme Court and, luckily, this thesis has not had further support.

systems. To force people to adopt and use a cryptographic system implies that the Government keep a copy of the key. This is actually a search or seizure in advance of any warrant.

Without all the requirements of either article 14 or article 16, there would be no possible opportunity for the Government to lawfully gain access to encrypted information, but in the following two cases:

The first is by adjournment of basic rights. In order to suspend the basic rights guaranteed by the Constitution, there must be an "invasion, a serious disturbance of the public peace, or [any other situation] that puts society in a serious conflict..."[272] Adjournment can only be established in these cases and exclusively by agreement between the President with all the State Departments Directors and the Attorney General, and by approval of the Federal Congress.[273]

Second, there is an exception to the legality guarantee of article 16, which is the flagrant crime.[274] Warrantless intrusion from the authorities into personal privacy is, otherwise, impossible.

Key escrow would apply either to business or people protecting or sending personal, commercial or political information, but, under the above mentioned circumstances, it would be very impractical for the Government to pursue a warrant for every key in order to, in principle, prevent crimes. Articles 14 and 16 would, hence, forbid the warrantless key escrow for private users of encryption, at least. Commercial users could perhaps be required to observe different rules, depending on the nature of their business and the regulations they are subject to.

[272] Article 29 of the Political Constitution of the United Mexican States, *Supra*, note 236.

[273] *Ibid.*

[274] Whether or not encrypted communications or information would constitute a flagrant crime is out of the scope of this work.

It is essential that law enforcement authorities can decrypt files because without that possibility it would be harder, if not impossible, for authorities to obtain evidence. At the same time, it is important that decryption be expeditious because the existing evidence could be sharply diminished, or even erased, as time passes by.

This is a delicate issue that has raised hot debates. To date, not even in the country of our comparative examples has file decryption played a significant role in convicting criminals. This issue is not solved yet and, at least in the USA, shows divided opinions between law enforcement supporters and civil libertarians.[275]

D) Constitutional Article 20 II: Compelled Speech.

Article 20-II enacts the prohibition of compelled speech, stating that in any criminal case "the defendant shall not be compelled to declare against him/herself".[276] The main problem here is that a mandatory key escrow would force the disclosure of something that the person would rather keep secret. This secret could even be sensitive or important commercial information, or something else not necessarily in connection with the cause that motivated the proceedings against the defendant. There is of course the requirement of having the presumption that the natural individual committed a crime and consequently should be under investigation,

[275] *See*: *supra*, (Anonymous) *Encryption: A Free Society's Dilemma*, *Supra*, note 83, at 6, stating that "...to dismiss predictions that what is now a minor inconvenience could turn into a very real problem for law enforcement and endanger our society in the future would be ...disingenuous and irresponsible." *See also*: D. Denning, "*The future of cryptography..*" *Supra*, note 172.

[276] Article 20, paragraph II of the Political Constitution of the United Mexican States. *Supra*, note 236.

in order for a case to fit this criterion.

Note that this article has never been construed in a sense that allows the Government to demand from individuals that they provide the circumstances that hypothetically would make future searches easy. This argument, it seems, would be completely against mandatory key escrow.

The first reason is that the obligation to disclose the chip key would be like requiring citizens to disclose private documents or papers. Second, the mandatory expression of the LEAF on each communication would perhaps be an incriminating testimony, which is forbidden by article 20 paragraph II. There is the question of fixing the limits of the possibility for a chip key or a session key to be "incriminating".

In this respect, there would be a delicate problem, not directly with the session or chip key itself, but with the LEAF because each conversation or communication has a unique session key, which is encrypted inside the LEAF. The LEAF precedes any conversation and can only be decrypted with the family key that would be in the power of the Government.

Thus, if the conversation that follows the LEAF were an incriminating one and if it happened that the authority were routinely decrypting LEAFs with the family key, there would be a substantial risk of prosecution.

Nonetheless, the Government would need a warrant in order to disclose the communication and legally begin the prosecution. The chip key disclosure may not, therefore, be directly protected against mandatory key escrow under the terms of article 20-II, but the warrantless use of that key to decrypt the LEAF would certainly be protected, although there is no other critical restriction established neither by Jurisprudence, nor by the text of the article itself.

The duress measures referred to in article 20-II have been interpreted by Mexican Courts as belonging to those that have an objective effect on the indicted's will.[277]

Mexican Jurisprudence has construed the verb "to compel" as "to obligate someone by force to do something he/she does not want to."[278] However, under the terms of the escrow system, the authorities would not have to *force* the presumed lawbreaker to disclose his/her key since it would be enough having a valid cause to ask the escrow agents to produce their parts of the chip's key to access encrypted data.

Could the competent authority otherwise compel someone to reveal the key to decrypt certain information? The key or password may be kept in the mind of the owner or in tangible means, such as in writing. If the key was only in the mind of the owner, it would be almost impossible to force him/her to disclose it since the owner will be protected by the terms of article 20-II: producing the key would establish the link between the suspect and the "incriminating" encrypted file.[279] If, on the other hand, the key was written down or electronically stored, the situation would be completely different, whereby the key would be protected only as a key to a box (as a possession) would be.[280]

[277] *See: Semanario Judicial de la Federación. Amparo directo* 44/90. November 14th., de 1990. Unanimity of votes. Reg. 6010, year 91, epoch 8.

[278] *See: Ibid. Amparo penal directo* 8437/37, April 20th., 1938, unanimity of 4 votes. T. LVI, p. 629. Reg. 1101, year 1938, epoch 5.

[279] *See:* P. R. Reitinger, "*Compelled Production of Plaintext and Keys*", January 16, 1996. Available online URL "http://law.lib.uchicago.edu/forum/ reitinger.html, sustaining that the keys should be observed as independent producible objects.

[280] *See: Infra,* Chapter III, part 3, section E), subsection i), when encrypted data is studied as a possession. *See also: supra,* (Anonymous) *Encryption: A Free Society's Dilemma:, Supra,* note 83, at 9.

E) Cryptography in Mexico: what analogy applies?

New technology poses problems for traditional law expressed in traditional language. Law often reacts to problems that can not be solved by virtue of its technological lacks by drawing analogies.[281] The most distinguishable example in this study has been that strong encryption software and hardware are considered munitions by some countries.[282]

The selection of the analogy has, and will have in Mexico in the future, crucial implications. We will focus on the possible approaches that a court could take to decide a case that involves encrypted information. Will encrypted information be treated as a security measure to protect one's possessions or as a possession itself?

Law in Mexico can not be applied by analogy, in principle.[283] However, the prohibition for the Courts to apply the law by analogy only concerns those laws that impose some kind of punishment, but it does not affect its application to procedural laws.[284] Furthermore, application of analogies is only forbidden in criminal proceedings.[285]

[281] *See*: M. A. Froomkin. *Supra*, note 15 at 859 through 882.

[282] *Cfr.* ITAR, 22 U.S.C. Sec. 2778 (1988 & Supp. IV 1992)*supra*, note 98. *See also*: J. P. Chandler. *Supra*, note 65, describing that in several countries import of strong encryption products is restricted, and that in some countries restrictions are the same that apply to munitions (for instance in South Africa, where strong encryption is considered an arm too).

[283] *See*: article 14 of the Mexican Constitution. *Supra*, note 236. This article states that in criminal cases it is forbidden for the Courts to impose, by analogy, any punishments that are not previously established by the law that specifically applies to the delict in question.

[284] *See: Semanario Judicial de la Federación, Amparo penal directo* 1443/32, September 11th., 1934, majority of 4 votes. T. XLII, Reg. 480, year 1934, epoch 5, p. 500.

[285] *See: Ibid. Amparo en revisión.* 236/93, September 2nd., 1993, unanimity of votes. Reg. 8639, year 1993, epoch 8.

i) Encryption as a personal paper, possession, or document.

Violation of articles 14 and 16 can only come from real deprivation facts that are already proven, and not from hypothetical situations.[286]

Administrative searches must satisfy the requirements of article 16 concerning search warrants. This does imply that administrative searches must follow certain formalities only. It means that they must follow the whole terms of administrative warrants. Thus, there is no reason to think that only searches that derive from criminal procedures shall observe those principles and mutilate this protection when dealing with searches that come from administrative procedures, because "the protection of the domicile privacy of somebody that is the suspect of a criminal case, does not warrant a higher level of protection than those individuals who are not."[287]

Search warrants are considered acts of annoyance by Mexican jurisprudence. Article 16 of the Mexican Constitution requires the investigative authority to submit to the citizen under investigation a copy of the written search warrant on which it founds its acts.[288] An escrow-based search would have to be necessarily based on both a valid judicial order so that encrypted information can be accessed, and a notification and requirement to the escrow agents to produce their parts of the chip key.

The fact that article 16 refers to "books and papers" does

[286] *See: Ibid. Amparo administrativo en revisión* 367/ 32, September 25th., 1933, unanimity of 4 votes. Reg. 586, year 1933, epoch 5, t. XXXIX, p. 538.

[287] *See: Ibid. Amparo en revisión* 1041/81, April 16th., 1982, majority of votes. Reg. 918, year 1982, epoch 7, Inform 1982, 3rd. part, p. 44.

[288] *See: Ibid. Amparo en revisión* 791/80. March 25th., 1981. Reg. 915, year 1981, epoch 7. Vols. 145-150, 6th. part, at 299, unanimity of votes.

not mean that conventional legislators can not establish some other methods of verifying accountant entries. It must be understood that by mentioning books and papers the intention of constitutional legislators was to generally refer to the administrative authority's ability of verifying any kind of accounting entries that a tax payer might have. Furthermore, there is no reason to suppose that the Constitution should mention all the possible ways under which tax payers can have registered their operations.[289]

Compulsory production of private papers is prohibited by the Constitution, if not made with the requirements of article 16. Arbitrary deprivation of papers (as a civilian possession) is also forbidden by article 14. Possession's constitutional protections are meant to secure the individual's documents which, if disclosed, may compromise him/her in any sense.

According to a jurisprudential thesis, the only requirement for considering something as a possession is the simple material tenancy of the thing itself,[290] but there is an area of debate as to the type of possession protected by article 14. The text of the article does not distinguish between the original possession and the derived possession, so we can conclude that it protects both.[291] What is important here is that possession, as stated in article 14, can then also consist in papers.

The denomination of "paper" referred to in article 16 of the Mexican Constitution comprehends all the documents of a certain person.[292] Thus, papers can be any written record of any fact, such

[289] *See: Ibid.* Mexican Jurisprudence Thesis number 6/1993. Mexico, City. October 8th., 1993. Antecedents: 1.- *Ibid. Amparo en revisión* 1111/92. July 1st., 1993, majority of 17 votes. 2.- *Ibid. Amparo en revisión* 247/93 July 10th., 1993, majority of 17 votes. 3.- *Ibid. Amparo en revisión* 367/93. July 10th., 1993, majority of 17 votes. 4.- *Ibid. Amparo en revisión* 587/93, July 10th., 1993, majority of 15 votes. 5.- *Ibid. Amparo en revisión* 1167/92, August 3rd., 1993, majority of 16 votes.

[290] *See: Ibid. Amparo en revisión* 704/88. March 10th., 1989. Unanimity of votes. Reg. 5478 year 89, epoch 8.

[291] *See*: I. Burgoa Orihuela. *Supra*, note 237 at 543.

[292] *Ibid.* at 595.

as personal records or information of any kind, but not tax-related documentation because there are some specific rules for it under article 16.

Encryption is not itself a paper, but obviously it is the means for keeping "digital papers" safe.[293] An interesting question here is to decide whether the key is also a paper, and if so, if it is independent from the other papers it helps keeping safe, or whether a key is a possession, a good or simply an idea.

These are questions whose answers will depend on whether or not the courts assume that an absolute level of privacy is a social good, and if so, to what extent the courts should order the production of the key or the production of the plaintext. Answers will also depend on the ability of the courts to face the problem of ordering the production of the key, because "the recipient of a subpoena or other legal request to withhold a key, ...can always claim that the key was lost, or even intentionally destroyed, before receipt of the subpoena or request."[294]

[293] We have to bear in mind that the public availability of strong (non-escrowed) encryption is a *de fatcum* situation that will certainly complicate the issue. *See*: P. R. Reitinger. *Supra*, note 279.

[294] *Ibid.* The author stresses that proving the continued existence of the key will in many cases be impossible, rendering encrypted information unavailable to law enforcement authorities. The author states that keys have the function of being intangible locks on electronic documents. As regards to the issue of "whether law enforcement can compel production of keys that are only known, rather than recorded, is an open question, but one that should arise infrequently because most keys will be recorded."

These issues, though, deserve separate investigations. For our purposes, it is convenient to remember the pertinent comments made on these topics above in connection with compelled speech [*supra*, Chapter III, part 3, section D) and E) subsection i)| which represent the main obstacle for law enforcement. For an excellent in-depth description of the theme, *see*: P. R. Reitinger, *ibid.*

ii) Encryption as a vehicle.

The word vehicle refers to the means of transporting something from one place to another. Encryption is not the means of transporting information or transmitting messages. This idea confuses encryption with one of the characteristics of the information highway itself. To only construe encryption technology as the means of transporting data would be as poor an analogy as to say that the information highway is only the means of transporting information.[295] If we accepted this analogy an encrypted message would either be another communication or the way in which the message travels. In both cases, encryption would be construed only in the way it is used to encrypt communications that flow through risky environments, leaving out its characteristic of being a method of encrypting stored data.

So, why is it important to study the analogy of encryption to a car? Because part of the argument of encryption as message flow has important implications that somehow appear to be true in a sense: non-encrypted telephone and e-mail messages can be intercepted and read with certain degree of ease.[296]

This analogy is dangerous because if we assume that encryption is a vehicle to carry information, then we would have to study and determine important things. First, administrative authorities are authorized to inspect the legal status of vehicles in the country, and their correct registration. Second, the administrative authority has the ability to seize vehicles without a warrant if there are elements that indicate that the vehicle has been involved in illegal activities or is not registered.

[295] *See* the comments previously made on this topic, *supra*, Chapter I.

[296] *See*: M. A. Froomkin. *Supra*, note 15 at 863. The author mentions that in the context of key-escrow one could say that the chip's unique key is like a license plate on the information highway. "If the reigning metaphor for use of electronic communications is that of the car on the road, it is but a small step to fixed or random checkpoints, and other minor electronic detentions."

As regards the former argument, courts would have a difficult time applying this analogy. In fact, the aim of those articles is to check if a certain "suspected" vehicle has complied with tax regulations. Regarding the latter argument, and assuming that courts could apply the analogy and try to "seize" encrypted data, the courts would face another serious problem: strong non-escrowed encryption may produce cyphertext that, in this sense, represents greater difficulties for the authorities to decrypt than it represents to seize a car.

An important argument against this metaphor is that seizure in Mexican law is the means re-establishing the legal order by provisionally seizing certain goods.[297] Thus, decryption of encrypted data would necessarily have to comply with the purpose of re-establishing the legal order in order to succeed. Such a situation is unlikely to occur outside of the criminal arena where, in a sense, analogies are forbidden.[298]

iii) Encryption as a different language.

Plaintext is text converted into cyphertext when the message or data are encrypted. Cyphertext is, as we know, unreadable if one does not have the key to decrypt the message. The question is then to decide whether cyphertext is language.

The question presents the difficulty of determining whether the characteristic of any language is to be "understandable" by anybody under its apparent form.[299] If we accept this option,

[297] *See: Semanario Judicial de la Federación. Amparo directo* 633/89. May 23rd., 1989. Majority of votes. Reg. 5078, year 89, epoch 8.

[298] *See*: *supra*, note 283.

[299] *See*: M. A. Froomkin. *Supra*, note 15 at 867 quoting a study by D. Denning, stating that languages share the property that "thoughts, emotions, beliefs,

cyphertext should be readable and understandable as such, in order to be considered *language*. Yet, we know that nobody can understand a ciphered message before decrypting it. Not even the person to whom the message is addressed can understand it before decrypting it with the correspondent private key. So, in this sense, cyphertext would not be language.

If, on the other hand, we reject the characteristic of language as being comprehensible under its apparent form, then cyphertext *is* language, since it contains the expression of someone's ideas. There is another supporting idea for asserting this: "[a]s new technologies such as voice recognition become common place, one would not expect to see arguments that the speech is somehow less protected while in the binary form that intermediates between waves and text, even if the author could have used a pencil instead of speaking to a computer."[300] In the end, the difference between text and binary text only concerns the use of a computer machine in order to transform it.

Accepting the analogy of cyphertext as a different language would yield two conclusions: all cryptographic systems would enjoy the same protection that foreign languages have in the country, and law enforcement authorities would have problems to force the translation of encrypted messages.

From the standpoint of language as free expression of ideas (freedom of speech) guaranteed by article 6 of the Mexican Constitution, the difference between cyphertext and plaintext would not be relevant since communications are protected as speech. The only limitations to the freedom of speech are good morals, rights of

requests, offers, and concepts can be expressed without knowledge of any other language." Besides, cyphertext must be first decrypted to be then translated into any other language. That is why Dr. Denning concludes that encrypted language is not language.

[300] *Ibid.* at 869.

third parties, public order and commission of delicts.[301]

iv) Encryption as a security measure.

Cyphertext can be comparable to a document kept into an unbreakable safe, whose key can be written down or not. However, there are some differences between a safe and cyphertext. For instance, if the safe consists of a gun case, it is surely not expected to be very private. By contrast, encrypted messages do not give any appearance away of their content, and so their expectations of privacy are not undermined by this reason.

Some might argue that encrypting a document prior to any investigation is much like burning or shredding the document, which equalizes criminalizing the use of encryption to making burning paper illegal. However, when one burns a document, it no longer exists and the user has no further utility in it. Conversely, when a file is encrypted, the contents remain useful to the owner. Hence, the file would more accurately be considered the same as if it were in a locked box for which the owner had the key (an analogy explained later), rather than a document that had been burned.[302]

It is not because things can be kept safe that they are out of the reach of law. As long as those things do not consist in self-incrimination materials, there is nothing wrong with asserting that its owner can be compelled to produce them if there is a valid cause

[301] *See*: *Semanario Judicial de la Federación*, t. XXXVIII, 5th. epoch, p. 220. For further reference on effective court decisions on these topics *see*: the Bernstein case description above, Chapter II, part 3, section C), subsection ii).

[302] *See*: *supra*, (Anonymous) *Encryption: A Free Society's Dilemma*:, *Supra*, note 83, at 6. The author estimates that "[i]t is wrong to consider decryption keys only in the context of safe combinations and strong boxes... it is imperative that we view encryption technology in a contemporary light."

for doing so.[303]

v) Encryption as an extension of the individual's *domicile.*

As a prolongation of individual freedom, the domicile can not be violated, except in the cases specifically established on article 16, *i.e.*, by virtue of a search warrant or an administrative search.[304] If the warrant is defective or if the authority commits an anomaly during the search, this is an issue that does not affect the norm itself. Warrants are in fact necessary for law enforcement.

Viewing encrypted data as a part of people's domicile, implies two things. First, encrypted data that are not supposed to be sent or communicated is a possession protected as the domicile itself is, in which case we would return to the paper and possession analogies.[305] Second, messages that are indeed intended to be sent to the outside world would deserve the same treatment as possessions once leaving their home source. As article 14 protects not only people but also places, the interconnected networks by which one's message reaches its destination would also be protected.

There is a number of difficult and interesting questions with this analogy. For example, how can law enforcement authorities conduct surveillance without invading one's privacy? What is a message once it has left its source? Is it still a paper or possession

[303] *See*: M. A. Froomkin. *Supra*, note 15 at 873-874.

[304] *See: Semanario Judicial de la Federación. Amparo Civil en revisión* 5779/38. March 21st., 1941, unanimity of 5 votes. Reg. 792, year 1941, epoch 5.

[305] *See*: M. A. Froomkin. *Supra*, note 15 at 878-879, stating that, in these cases, "strong cryptography would provide a nearly unbreakable means of protecting one's private papers stored in the home computer."

of the sender that deserves the treatment that his/her home receives? Is it something else?

vi) The ability to decide on the analogy.

As stated at the outset of this study, the challenge for current Mexican law to respond to the new conditions on communication media is a difficult one. The answers that the Mexican Congress and courts will give to these questions will shape not only the legal arena, but also the bases on which people will decide whether or not to trust their personal and commercial interests to the information highway. From the menu of analogies described here, some are likely to favor either law enforcement or personal privacy interests.

The Mexican courts and Congress have to come to grips with the legal implications of cryptography. We can conclude that out of the criminal area, where analogies are forbidden, Mexican courts and Congress will face the need to decide how to treat encryption programs and encrypted information. The Committee will find it useful to study the analogies proposed here in order to advise the Congress on the question. The Committee should consider that the language and freedom of speech analogy gives a strong support for individual privacy interests, but presents some inconveniences for law enforcement authorities. By contrast, the car on the superhighway analogy seems likely to provoke a lower level of privacy for individuals and provide higher investigative abilities for authorities.

The analysis of this variety of analogies will be of extreme importance since it will help shape the answer to the debate between law enforcement and privacy protection. What is even more important is that this analysis will drive lawyers and people involved in future law making on these issues in Mexico to re-evaluate the meaning of the Constitutional principles of privacy, lawful security and law enforcement.

CHAPTER IV. FINAL RECOMMENDATIONS AND CONCLUSIONS.

1. Encryption facts and their implications for Mexico. Recommendations for the Committee.

- *Online risks and the role of encryption*
- *Laws on encryption in the world and in Mexico*
- *Law enforcement against personal privacy: a debate.*
- *The size of the keys.*
- *Criminal use of encryption.*
- *Is escrow the answer?*
- *Towards a Mexican encryption policy.*
- *The need for a comprehensive legal framework on new communication technologies. Legislative recommendations.*

2. Legislative Proposals and Rationale.

- *Proposal on the promotion of the use of cryptographic technologies of privacy protection, message authentication and confirmation of the parties on a communication.*
- *Proposal on encryption treatment.*
- *Legislative proposal on choice of encryption system and key length.*
- *Legislative proposal on criminal use of encryption.*
- *Legislative proposal on lawful compulsory decryption on criminal cases.*
- *Legislative proposal on key escrow.*

3. Conclusions.

4. Epilogue.

5. Graphs.

CHAPTER IV. RECOMMENDATIONS AND CONCLUSIONS.

This chapter brings together the conclusions drawn in the past sections of this study and makes recommendations to the Committee.

In the first part of this chapter, we describe the problems that encryption may solve in the online world and advise the Committee to take action to promote the use of encryption technologies in Mexico. Second, we outline some problems that encryption use may pose: its status, the difficult border between personal privacy protection and national security preservation (and the consequential debate that arises here), and the role of the key size. Third, we examine the problem arising as a result of the criminal use of encryption, and whether the courts should allow decryption or rely on a key escrow system to preserve law enforcement and constitutional rights, especially self incrimination. Fourth, we discuss the elements that an encryption policy should comprehend in Mexico. Finally, we emphasize the need for locating the encryption policy within the borders of a comprehensive legal framework on new communication technologies in Mexico.

Following the description in part 1, in part 2 we make legislative proposals on privacy protection through encryption technologies, the treatment of encryption, key size choice, regulation of the criminal use of encryption, decryption and self incrimination, and we outline the revision to communication law in Mexico.

Part three includes the conclusions stemming from this study.

1. Encryption facts and their implications for Mexico. Recommendations for the Committee.

Online risks and the role of encryption.

The world is becoming "smaller" thanks to technological advances that bring to our finger tips information, voice messages, music, and all kinds of data from almost any point of the globe. Almost all of today's transactions may be, or are in fact, conducted electronically. This high level of comfort implies serious potential risks for privacy, such as wiretapping, interception of wireless communications and other intrusions. Encryption technologies may provide an efficient solution to these problems, by ensuring that only the intended receiver may disclose the contents of encrypted information.

Increasingly, encryption technologies ensure the privacy of personal, commercial and governmental data. Encryption is playing an essential role in protecting our electronic privacy against threats from a variety of potential attackers. This solution, however, is not eternal or completely error-free. The two main potential "weaknesses" of this solution are, first that people have to take very good care of not losing or compromising their keys, because in this case even the best encrytpion technological method becomes useless; second, one must be aware that brute-force attacks against cryptographic systems once considered adequate are today both fast and cheap.

Mexicans are beginning to use encryption technologies, and it is important that the Mexican Government assumes its role of promoter of the use of these technologies,[306] foresees the problems that may arise from criminal use of encryption, and sets forth the basis on which to protect society from it. It is the mandate of the Consultant Committee on Informatic Policies to advise the Government, through the INEGI, on these issues and on the implementation of the IDP, and to assist the Congress on its assignments.[307]

Laws on encryption in the world and in Mexico.

All around the world, law faces important challenges with the rapid spread of encryption technologies. As far as encryption benefits are concerned, Governments have a very hard time defining the border between the protection of privacy and the potential threats such a protection poses to law enforcement. Even defining what exactly encryption is seems to be problematic, and answers to this problem are often phrased in terms of metaphors. Even encryption "keys" is a metaphor.

For some countries, strong encryption technologies are munitions that should be banned from export or import. For others, these technologies are potential tools to industrial development. For some courts, encryption and encrypted data are speech, whereas for other courts encryption is only the means of commanding a computer to perform a function.

In Mexico, this scheme is not yet decided. From the menu of metaphors we have analyzed, the "possession or document" and the "domicile extension" metaphors fall under the protection of constitutional articles 14 and 16 on one's private papers stored in the home computer. The classification of the cryptographic key as a

[306] As President Zedillo has stated on the National Development Plan, *supra*, note 182.

[307] *See*: *Supra*, Chapter III, part 1, sections B) and C).

private paper located in the home also may have important legal consequences and may drive us to reexamine what constitutes the "inside" of a home. The metaphor of "language" also offers great protection of privacy, although it may conflict with the abilities of investigative and intelligence agencies. The "security measure" metaphor is fairly unsettled since encrypted files may be considered as if they were inside a locked box of which the owner has the key. Thus, they are not out of the reach of the law since the owner can be compelled to produce the key if there is a valid cause for doing so. Finally, the metaphor of "car" is the most convenient for authorities concerned with electronic eavesdrop.

The choice of metaphor has important outcomes. The most evident one today is that strong encryption export is frequently controlled by virtue of the prevalence of the "munition" metaphor. For the moment, Mexico does not have to worry about exporting encryption, but it is time to prepare the legal field to comprehensively regulate encryption. This is one of the most important tasks that the Committee will have to face. Luckily, the Committee may take advantage of other countries' experiences with encryption, and encourage studies and consultations on these crucial topics.

The Committee should weigh the consequences of whether or not encryption should be treated as a munition. If it did, such a decision would imply the problem of building a classification system of encryption programs according to the strength of their algorithms and the size of their keys in order to separate "military-grade" encryption from "common" encryption, eventually yielding the prohibition of the use or import of the former. We have stated that akin systems that have emerged in countries that *produce* strong cryptography (France or the USA) have shown that those classifications are fruitless and that the ban on use and export is often unenforceable (since both may conflict with constitutional protections). Thus, our advice to the Committee is that it should study the consequences of the use of the analogies we have described, reject the treatment of encryption as a munition, and promote the use of the analogies that favor privacy protection.

Law enforcement against personal privacy: a debate.

Encryption control raises many important questions that can only be answered through analysis and consensus. The use of encryption creates a debate between civil libertarians and their governments. Let us recapitulate the legal initiatives representing the two poles that, to date, have been the interactive forces in defining the first legislative efforts to regulate encryption.

Governments' initiatives are based on a philosophy of national security. The State has to protect all the citizens from harmful use of communication channels. Therefore, Governments propose to control the import and export of encryption products. Some countries even control domestic development and use of encryption technologies claiming national security protection.

On the other hand, citizens' proposals are based on a philosophy of individual freedom and privacy protection. They point out that although law enforcement agencies declare that society, through national security, greatly benefits from these electronic eavesdropping activities, the extent of this benefit is unclear, considering past abuses and the likelihood of future abuses. Their initiatives have mainly been to prevent the Government from limiting export, import or use of encryption,[308] imposing any mandatory system of encryption, or requiring a copy of everybody's keys. These proposals have insisted that it should be up the individual to decide about the encryption program and key length of his/her choice.

The Committee should examine all these different

[308] Another point of this debate, in the USA arena, is (indirectly) the size of the keys, which is described below, since the Government restricts the export of encryption programs whose keys are bigger than 40 bits, but -for obvious reasons- allows the export of EES which uses a 128-bit key.

approaches: on the one hand, the beneficial uses of encryption and the promotion of its use and the prevention of the criminal use of encryption, and on the other hand, the protection of society. In addition, the Committee should evaluate these two extremes, encourage debate over them in Mexico, and propose a balanced solution that defines "privacy" and "national security", as well as the extent to which the State will intervene in protecting both of them in a coherent manner.

The size of the keys.

An important area of concern in the debate is the size of the keys. Bigger keys pose greater problems to intelligence agencies since they are more difficult to break. In general, programs that use keys bigger than 40 bits are restricted for export. Some countries even restrict the export of encryption programs that use 56-bit and bigger keys, whenever they are provided out of an escrow scheme. Just as the export controls have failed to stop the worldwide spread of strong encryption, attempts to limit the size of the keys will be fruitless.

The decision of which algorithm and key size to use in Mexico must be made now, and it should be made (and keep being made), by the users. From this standpoint, the Committee should ensure that Mexicans continue to enjoy this freedom and that no future law can restrict this right.

Criminal use of encryption.

Encryption use is completely justified, but its criminal use represents a significant threat to society. Strong encryption may protect drug dealers, organized criminals, bombers, kidnappers, etc. under secret identities with the same efficiency as it can protect the privacy of honest people and industrial entities. This has been recognized in other countries by both parties to the debate, Governments and encryption users, and there have been proposals from both sides to punish criminal use, or abuse, of encryption. Therefore, sanctions on this use of encryption appear like a vital component of any future encryption policy emerging anywhere.

However, the problem of decrypting files in cases where encryption technologies have been used to further the crimes is still unsolved. The two main difficulties with decryption are, first to decide which authority will have the ability to order decryption: state prosecutors, law enforcement officials or judges; and second, the extent to which this authority will be entitled to require the decryption of files without harming one's right to privacy. As regards the former problem, previous efforts to give administrative authorities power over privacy intervention (as TTPs) have been clearly rejected since the executive has been the promoter of systems that favor it with important eavesdropping abilities. Therefore, the best solution seems to be to give the ability to compel decryption to judicial authorities. Investigative authorities should solicit the judges to order the decryption of certain individual's files which, according to their investigation are necessary to follow criminal action against, or even convict, suspected individuals. The judges should decide whether such a request is justified. The second problem is even more delicate. An individual is not a criminal, whose privacy can be lawfully disturbed by mandate of law, until it is proven so in court. This fact presents one important objection: encrypted information could consist of part of the evidence necessary to press charges against criminals or even convict them. Yet, would it be justified that courts force an individual, who is merely under investigation, to decrypt his/her files? What would happen in cases where decrypted information was found to be irrelevant to the criminal investigation? What would happen in cases where the information was found to constitute a different crime from what the authorities were investigating? Would this be unconstitutional compelling of self-incrimination? These are some of the questions that courts will face, and that remain unsolved.

Two things must be taken into account at this point. First, obviously not *all* criminal evidence is susceptible to encryption. Yet, this is not reasonable enough to allow a "partial violation" of privacy, by practicing warrantless or unlawful decryption. Second, not all crimes represent the same potential dangers to society. Courts would surely be more concerned about decrypting the files of a suspected bomber than decrypting information of a minor tax-law infractor.

From this point of view, the elements that draw towards a solution will have to include a systematic crime differentiation, such as the one proposed by the latest criminal law reform in Mexico which is meant to control organized crime. In any case, this solution implies a re-evaluation of the principles of privacy and security, their consequential constitutional protection and their limits. The parameters under which regulation of decryption is decided can make a difference between a "law enforcement-personal freedom" balanced system and one that is not.

For instance, we have seen that imposing control over encryption spread through the establishment of *de facto* standards was not a poised solution. On the contrary, these standards have raised several constitutional objections. Creating encryption standards is not an inadequate idea, but it should be a decision reached by consensus between the Government and its citizens.

The Committee should rapidly address the issues described above and propose the limits for decryption in Mexico. Our advice here is that the Committee recommend a crime differentiation treatment system that helps the courts decide whether to allow decryption, for which cases and to what extent.[309] However, this

[309] The new criminal system makes a differentiation like the one proposed here, by classifying which delicts represent organized delinquency -and therefore should be treated differently. *See*: Constitutional article 16 (*supra*, note 236) stating that the "indicted's" arrest, which is practiced by the "Judicial Public Representation" (*Ministerio Público*), can not exceed 48 hours, except in those

solution can not stand alone. It will have to be supported by a constitutional reform that clearly establishes the limits of personal privacy and the specific circumstances under which it can be disturbed. The latest constitutional reform to article 16, which was supposed to have given the basis to fight organized crime, added little in this respect.

Therefore, the new needed regulation should consider the special cases in which decryption can be ordered by the courts. In order to avoid claims of "privacy" violations, the new system should ensure that first, decryption will only be authorized by the court; second, that decrypted information will not be disclosed by the judges to the investigative authorities, and will be kept by them as a professional secret, if they decide that such information is not relevant to the ends of that investigation, is not related with it or constitutes merely private information.

The system we propose to the Committee will achieve two things of paramount importance: first, it will assure prompt access to encrypted information, which is one of the most important concerns for law enforcement authorities; second, it will ensure to the person under investigation that no information of his/her property that is not directly connected with the facts of the investigation will be disclosed to anyone.

Note that this system will ultimately leave decryption in the hands of the "effectiveness" of the warrants, and that warrants will not always necessarily achieve decryption of the information if the "indicted" party refuses to decrypt his/her information. This is a problem to be solved yet. Until a better proposal emerges, this will be the risk that almost all compulsory decryption systems will run. One could argue that escrow systems do not pose this difficulty, but the answer to this would be that escrow systems may pose other, and from our point of view greater, objections.

cases established by the law as organized delinquency, where this term can be the double.

Is escrow the answer?

Some Governments (like the USA) see in escrow the solution to ensure that no information will be running the risk of being intercepted or disclosed by "anybody". Escrow systems (such as EES) provide a 128-bit key that is long enough for protecting electronic data for a long period of time against almost any type of attacker having the resources available today.[310] Besides, with escrow, the authorities could decrypt files without having to order the production of anybody's key. Escrow systems have received some support internationally and even the OECD Meeting recognized that escrow may be a balanced solution to regulate encryption internationally. So far, escrow systems seem to be a very good option to solve the debate.

There are, however, strong objections against these systems which we recapitulate below.

When the Government wants to investigate someone, it will request from the TTPs not only the chip key of the individual it wants to investigate, but also the chip key of anyone who has contact with that person and whose conversations are being wiretapped. This represents an enormous risk for the people who are not under investigation since their keys are being collected because of an *indirect* reason by the government agencies.

Escrow systems, as they stand today, mean that the Governments generate the keys for everyone. Therefore, there are also very important concerns about the scarcity in legal guarantees for unlawful invasions on privacy, as well as in remedies against the escrow agents that act negligently or fail to follow their own procedures.

Moreover, escrow systems are mainly produced in countries

[310] *See*: recommendations on the study of Blaze, M. *et al. Supra*, note 64.

that have tight export controls over encryption products other than escrow. Hence, there are serious concerns with the system these countries will adopt to export escrow to other countries. The most important concern here is whether the producing country will ask to keep a copy of all the exported keys, or what system will be followed to both, preserve the safety that escrow is meant to give, and ensure the importing country that no other foreign authority will have a copy of its citizens' keys and that, therefore, its national security will remain untouched. This is a question that remains unsolved yet in all escrow systems.

From the point of view of the Mexican Constitution, there are also important objections that are worth mentioning again.

Firstly, compulsory escrow would conflict with article 6 because the system would result in forcing people to conduct their private communications through a specific channel, pre-decided by the Government, *i.e.* escrow. Furthermore, we must remember that the only limit to expression of ideas is the commission of a delict. Thus, mandatory escrow would violate article 6 since it would equal to restrain the means for expressing ideas.

Secondly, mandatory escrow would violate constitutional article 7. The reason is that freedom of speech and press mean freedom of thinking and acting, and freedom of acting can only be limited if it threats the social order stability, the institutions, the public peace and other people's rights. Compulsory escrow legislation would apply to communications, regardless of their contents, and this could be construed as a restraint to freedom of speech. Moreover, compulsory escrow includes a high degree of individual identification, which goes against the anonymity that parties to a communication would often like to have. Furthermore, compulsory escrow may complicate the associational freedom of people who want to gather but would rather keep secret their participation in certain associations.

Thirdly, compulsory escrow faces serious barriers with constitutional articles 14 (Guarantee of lawful security) and 16 (Guarantee of justice). The difficulties for the Government would begin whenever it would need to decrypt information that presumably is in connection with a determined crime. In this case, the Government should initiate a lawsuit against the "indicted" party, win, and then obtain the warrant or authorization from the judge to ask the escrow agents to provide their parts of the chip key. Then, these two parts would be joined which would eventually lead to the disclosure of the contents of the message. This represents a substantial delay that criminal investigations can not be subject to. Moreover, the terms of both articles forbid the warrantless key escrow for private users of encryption, at least; commercial users could perhaps be required to observe different rules, depending on the nature of their business and the regulations they are subject to. The second objection is that article 16 subordinates criminal responsibility to the freedom of the individual, but does not demand that the people participate in the *creation of the conditions* that make searches and seizures effective. Under this line of thinking, citizens would be protected by article 16 against mandatory escrow even if the Government would have the lawful authorization to search in someone's possessions or papers.

Finally, constitutional article 20-II also represents an objection against compulsory escrow from criminal defendants since it could constitute an issue of compelled speech. The reason is that such a system would force the disclosure of something that the person would rather keep secret and that, besides, could also be completely unconnected with the cause that motivated the proceedings. Moreover, this article has never been construed in a sense that allows the Government to demand from individuals that they provide the circumstances that *hypothetically* would make future searches easier. Besides, the mandatory expression of the LEAF on each communication encrypted with escrow (under the EES system previously examined) would perhaps be an incriminating testimony whose compulsion is forbidden by article 20-II.

Furthermore, the warrantless use of the family key to decrypt the LEAF would be a violation of article 20-II since it would have an objective effect on the indicted's will, would obligate this individual to do something he/she does not want to do, and would establish the link between the suspect and the "incriminating" encrypted file.

To decide whether or not to adopt an escrow system in Mexico, the Committee should evaluate all the potential difficulties that these systems represent today abroad and also make a diagnosis of the domestic constitutional objections described. Here it should also consider that either importing an escrow system or adopting an international commercial escrow system would conflict with basic principles of Mexican constitutional law. Our advice to the Committee is to explore other non-escrow schemes of protecting domestic law enforcement concerns, and to follow instead a decryption system such as the one proposed above.

Another advice to the Committee is join International efforts that are being carried out to adopt an international encryption standard, which to date seems to be pointing towards escrow. The next OECD Meeting in Canberra next February 9th., 1997, is a good opportunity for Mexico to start this journey. This Meeting will be extremely important since it will probably determine the future global perspective on encryption regulations, considering escrow systems as the proposal of an international standard. Mexican law will certainly benefit from this contact and the experience will help tailor a national balanced encryption system that is suitable for both sides of the debate.

Towards a Mexican encryption policy.

Do we need to invade individual freedom in order to fight organized crime? If so, how much invasion is necessary? What protections should be granted to these invasions?

We pointed out above that encryption used by criminals is a potential threat to society and that the Governments should provide the means to protect their citizens from the criminals that can hide their identities under encryption technologies. We have stressed that an efficient decryption system is essential to this process. The two answers examined here, and that are available today, are: First a system that leaves some degree of uncertainty for law enforcement authorities in cases where the supposed criminal refuses to decrypt his/her data, which is the system we advocate. Second, the escrow system, against which greater objections can be voiced. As we can see, important aspects of problems raised by the use of encryption technology (criminal use of encryption and lawful decryption) remain unsolved and represent potential perils for societies.

There is no absolute answer to the questions outlined above, but there are some paths that can be explored to solve them.[311]

For instance, Mexican law is now going towards a future regulation of lawful surveillance of voice and data communications of people pertaining to organized delinquency groups. The Government has expressed its concerns about prosecuting particularly "serious" crimes and has managed to mold them within the last criminal law reform. An important and debated aspect of this reform addresses communication detection by investigative authorities. There was something, however, that was not on the legislators' minds when they shaped this reform: detection of communications will be much harder, if not impossible, if they are encrypted with strong cryptographic technologies. This would turn future wiretapping by Mexican law enforcement authorities virtually fruitless.[312] A further fact must always be taken into account in this

[311] To avoid repetition, we refer the reader to our concluding comments on these two topics. Next, we will review our comments on the last reform to the Mexican criminal system and will analyze whether it will be of any help to solve the problems outlined. If not, we will define what elements of solution will help in this respect.

[312] For an example of encryption use by criminals *see*: (Anonymous) *Encryption: A Free Society's Dilemma*, *Supra*, note 83 at 19, describing a criminal case where a pedophile used a military-grade encryption system to encrypt files

issue: as long as there are strong cryptographic algorithms freely available on the Internet, Governments will have to face important legal and technical obstacles to comply with their law enforcement and national security protection mandates.

Today, there is no legislation that makes it illegal to use strong cryptography (except in the specific cases described in the comparative studies of Russia and France). An important argument that supports this idea is that encryption is not the key *per se* .[313] This poses the delicate problem of defining which uses of encryption should be punished and how to limit their sanctions. The problem is delicate because "[i]t is unsettling to think that one's rights may turn on the extent to which people are able to find a technological means to defeat what would otherwise be legitimate government action."[314]

Following these ideas, the Committee will have to make its recommendations in harmony with the existing control over organized crime. The Committee needs to define the limits to privacy invasion that this new comprehensive system should allow and depend on. The criminal law reform is an example of the methodology used to differentiate between crimes, decide which deserve special treatment and decide how much invasion is necessary. Protections to these invasions, we suggest, can rest with the judges.[315]

There are, however, important connected elements that the Committee will have to analyze because the framework that

that the US police suspect contains a diary of his contacts with young boys all over the country.

[313] *See*: D. Denning, "*The future of cryptography..*" *Supra*, note 172.

[314] *See*: M. A. Froomkin. *Supra*, note 15 at 881.

[315] *See*: *Supra*, (Chapter IV, part 1, "criminal use of encryption"), where it is pointed out that judges should exclusively be in charge of analyzing the contents of decrypted information that is presumably in connection with a delict commission in case it is not, judges should keep this information out of the reach of investigative authorities, protecting it as a professional secret.

regulates encryption is fragmented. Thus, encryption policy in Mexico can not emerge alone, but as a constituent of a review to those bodies of law that relate to communication technologies.

The need for a comprehensive legal framework on new communications technologies. Legislative recommendations.

We have pointed out the reasons why the Mexican legal system will have to recognize both the illegal and the beneficial uses of encryption and build a legal and administrative infrastructure that protects society from abusive and negative uses of encryption technologies, as well as from arbitrary governmental intrusions into people's privacy.

We will now state the modifications we propose to Mexican Legislation, based on the study have made of this topic on Chapter III, section 2.

Constitutional principles and doctrines are often challenged by rapid technological changes. They provide the opportunity of rethinking constitutional doctrines that have been considered comprehensive for a long time, and of examining their coherence. The interpretation of constitutional principles changes as social realities evolve. It is essential that Governments and their citizens rely on a clear definition of the meaning of privacy and national security. These two principles are often opposed, mostly to the detriment of people's privacy. National security and law enforcement reasons are often claimed by Governments to commit acts against their own citizens.[316] This struggle sometimes occur within lawful parameters, and this may result in people trying to defeat what can be a legitimate government action.

[316] This is one of the main reasons why Human Rights protection associations are created.

The two principles of privacy and national security are unfortunately not clearly -or directly- defined in the Mexican legal system. Personal privacy is not defined *per se;* it is only defined by the guidelines that the Mexican Constitution sets forth and that authorities should follow to respect privacy, or at least not to violate it. National security is not directly defined either. The Constitution establishes that the basic rights' only limits are the respect third parties' rights , public order, the commission of delicts, and sometimes good morals. We might wonder whether this represents the "backwards definitions" of National Security. Moreover, there is now a system in Mexico that fights organized delinquency, and that was motivated by the need of having the constitutional and criminal law bases to control these organizations, whose great economic power and violence capabilities pose a serious peril to Mexican society. This is a more defined feature of National Security, but now the question is: is National Security the same as protection of the collectivity?

Another problem is that outside the spectrum of citizens' privacy violation by their own Governments, personal privacy protection and National Security safeguarding should not be considered as necessarily opposed. On the contrary, in the context examined here, personal privacy should be considered as part of the State's mandate of protecting National Security. In fact, the more these two principles are separated, the harder it is to balance them. To approach them as a whole is perhaps helpful to achieve a poised solution.

The Committee should address the imminent need of defining these two fundamental parts of the legal system within the context of the information revolution, and draw the line between these two principles that conflicts remind us exist.

Regarding the *Federal Public Administration Act,* there are some problems that the information revolution poses. Information technologies may be incorporated in almost any aspect of human activity and, therefore, many authorities can have jurisdiction -and many laws can be applied- in a single case. This administrative and legal fragmentation of the surroundings of new communication technologies dilute responsibilities of the authorities and makes it harder to design national strategies. Some way of consolidating responsibilities is necessary. Yet, it is impossible that a *single* Ministry should treat them systematically.[317]

The Committee's recommendation is to create an Inter-secretarial Commission on Informatics, a National Office for Policy, an Inter-secretarial Committee to Follow the Fulfillment of the IDP, a Federal Public Administration Committee of Authorities on Informatics, and an Informatics Committee on State and Municipal Public Administration. We believe that this is the most viable solution since it ensures that all the social sectors participate in the fulfillment of the purposes of the IDP.

The recently enacted *Federal Telecommunications Act* mentioned the existing connection between telecommunications security and sovereignty of the Nation, and defined what the terms telecommunications, private and public telecommunications networks mean. It established that all telecommunications networks are "general communications channels" for the purposes of the General Communications Channels Act. Both these precisions are positive. It also punishes the interception of information transmitted through public networks. As for the term National Security, it was indirectly mentioned regarding the dispositions that refer to

[317] To illustrate this situation, it is useful to remember that national security protection is an attribution that is shared by the Ministry of National Defense, the Mexican Navy, the Mexican Army, and to some extent the Ministry of the Interior. The technical perspective of information technologies in Mexico is slightly better defined as a responsibility of the Ministry of Communications and Transports. Promoting commerce and economic development, regulating industrial property, transferring technology, and establishing restrictions to the import or export of certain goods is an attribution of the Ministry of Commerce and Industrial Development.

requisition, and when the Act reserves the use of some satellite fields for National Security purposes. Unfortunately, the Act left important gaps. It did not mention any specific protections concerning user's privacy on telecommunication channels, and against unlawful intervention of the Government. It did not address the terms protecting National Security on telecommunications flow, either and it did not mention cryptographic technologies at all.

Therefore, the Committee should study the pertinent amendments that this law requires. We propose that it should consider among other things, the use of cryptography[318] by telecommunication channels users as one of the possible measures to protect their privacy and to ensure the authenticity and integrity of their messages. It should also think about a differentiation between the beneficial and the criminal uses of these technologies, and the prohibition of the latter.[319]

Regarding the *General Communications Channels Act*, there is nothing to add since it only applies to postal service routes and telecommunication networks today, and is limited to those cases that are not covered by the specific legislation, *i.e.* the above-mentioned Federal Telecommunications Act.

As for the *Criminal Code* and the *Code of Criminal Procedures*, today there is no disposition that allows or regulates private communication intervention, nor are there any guidelines concerning the protection of electronic data. The recent reforms introduced to both Codes added little for our purposes since

[318] It is useful to remember here the recommendations we have made regarding the analogy that should prevail to treat encryption.

[319] The parameters of the proposals are detailed farther on. *See*: *Infra*, Chapter IV, part 2.

neither regulation of crimes *online*, nor the protection of privacy on public networks, and of data electronically stored or sent were mentioned. Therefore, one can conclude that legislators were not concerned with information technology in these reforms.

The only part of the reform that is of interest in this study, is the definition in the Federal Code of Criminal Procedures of the term "organized delinquency" and the crimes to which is applies: terrorism, sabotage, piracy, prisoner escape, attack to federal channels of communication, unlawful utilization of air transit installations, crimes against public health (drug-related crimes), rape, hijacking, murder, kidnapping, some cases of aggravated theft, bribery, and some cases of arms traffic.

This crime classification, along with its differential constitutional treatment, is the systematization upon which we propose to regulate decryption. The decision of the judges on whether to order decryption should always be prompt. These special cases, however, require an especially expeditious judicial resolution of the decryption request from investigative authorities, who -if the judge so decides- will order immediate decryption, following the guidelines of the system we propose.

In this line of thinking, the two Codes should state that decryption will only be practiced by judicial order and that decrypted information will only be disclosed to the investigative authorities if it is relevant for the purposes that the request establishes. Otherwise, decrypted data will be returned to its owner and judges will keep the information they know about the "indicted" as professional secret. Resolutions on decryption requests in those cases defined by the law as "organized delinquency" should be taken into account as a priority and, therefore, be decided by the judge in a short term. This could be 24 hours, if we follow the term that the Code of Criminal Procedures recently adopted for the judges to decide authorization on seizures in cases of organized delinquency.

Finally, concerning the *Federal Act on Fire Arms and Explosives* and its *regulations*, we do not think that approaching encryption technology as a munition would be the most suitable of all metaphors, even though we admit that encryption is a personal security measure, as arms are.

In Mexico, considering encryption technology as a munition would imply building a system that distinguishes military-grade from common-grade encryption and punishing unlawful military-grade encryption use or import. This would equal to restrict the freedoms of choice and domestic use of encryption. There are strong objections against such controls on encryption use, as we have pointed out. Moreover, controls over encryption import, export or use have proven to be, at the end, unfruitful.

As we have emphasized, there are important gaps in Mexican law. The Committee should recognize that the section that refers to information technologies is almost completely barren and that there is a need of a comprehensive reform of the legal and administrative infrastructure of information technologies. The recommendations we have stated above may be useful in this journey.

2. Legislative Proposals and Rationale

The following proposals give some initial legislative guidelines on the topics analyzed all through this study and will help achieve the much commented balance spectrum for the Mexican encryption policy.

Proposal on the promotion of the use of cryptographic technologies to privacy protection, message authentication and confirmation of the parties on a communication.

The Consultant Committee on Informatic Policies should promote the use of cryptographic products so that Mexican citizens, enterprises and governmental institutions can benefit from the advantages that these technologies offer to electronic information. Encryption technologies should be promoted to protect information electronically stored or sent through data networks. Digital signature technologies should be promoted so that the parties on digital communications can ensure the source of the data transmission and the authenticity of the information transmitted.

Rationale:

Cryptographic technology is one of the main ways of achieving goals that are essential to digital communications in the world today: that the identity of the subjects on a digital communication is certain and that transmitted information is not altered on its way, and that data stored or sent through insecure channels can only be disclosed by the person to whom the communication is addressed, and not by anyone else. Digital signature and encryption provide the solution to these concerns. Their worldwide role in promoting industrial and commercial development is becoming more important every day. Therefore the Committee should promote their use in Mexico.

Proposal on encryption treatment.

The Committee should promote the treatment of encryption technologies as a security measure. Encrypted data should be treated as a private document or paper and data stored on the home computer of an individual should be protected as any other possession of his/hers. The Committee should also recommend the abstention from the Mexican Government of treating encryption as a munition.

Rationale:

Encryption is a term that suggests some metaphors: its hash functions "disguise" information, so that it can only be interpreted by the person who has the corresponding "key"; strong encryption systems are considered "munitions" since they are perceived as potential threats to authorities; the algorithms that encryption programs use to accomplish their functions are either "speech" or "commands" that a computer receives to perform an operation.

We have analyzed a number of metaphors that provide different advantages and disadvantages for authorities and individuals, and we recommend that the Committee promote the use of those metaphors that ensure that constitutional Guarantees remain intact. The prevailing metaphor that relates to encryption today is "munition", one from which Mexico should stay away. This metaphor has emerged as a result of the US and French belief that it will discourage export of cryptographic products and therefore will control its diffusion worldwide. The adoption of this criterion in Mexico would result in unfortunate outcomes, *i.e.* encryption would be subject to import and domestic use restrictions.

Legislative proposal on choice of encryption system and key length.

Any Mexican shall have the lawful ability to choose, use, import, export or develop any encryption or data compression system, regardless of the algorithm and key length selected and of the medium used.

Rationale:

Encryption use is not restricted under the terms of the present legislation in Mexico. Under the philosophy of a "State of Law" (*Estado de Derecho*), all the activities that are not specifically forbidden to the citizens are therefore allowed. On the other hand, the State can only act within specific regulations. However, there are many examples that have shown that there are areas where this protection is not enough. The area of information technologies -and specifically encryption- should be no exception. Furthermore, information technologies can be part of almost any aspect of human life and, thus, their possibilities of entering into conflict with the attributions of a governmental institution are larger, specially with national security concerns. A system that expressly protects individuals from abuses from the public powers will always have more chances of being trusted, than a system where individuals should guess whether their behavior would somehow infringe the law. A legal framework that clearly states the rights Mexicans have concerning encryption will have greater chances to achieve the beneficial ends that encryption can offer than a system limited to a mere non-prohibition.

We propose that the Committee work on evaluating the implications for each of the different beneficial purposes that encryption provide, and *recommend* which are the sizes that are ideal for each encryption use. We insist, however, that the final decision be left in the hands of the user.

Legislative proposal on criminal use of encryption.

Mexicans' freedom of choice of use, import, export or development of encryption or data compression systems shall only be restricted in cases where these liberties are proven to have been used to further crimes, as well as in cases where the law establishes as organized delinquency. People who are found by a court to be involved in a crime furthered with the use of encryption technologies or that are found to belong to organized delinquency, shall be subject to the restrictions that the authority establishes. Such restrictions will include asking permission from the authorities to further import, export or development of encryption products. As regards their further use of encryption, these individuals shall be subject to the escrow restrictions established by the authority.

Rationale:

Since strong encryption can be used by everybody, including criminals, disguising information in a way that makes its access almost impossible by strangers to these data, it is necessary to regulate its criminal use in order to protect the society and provide the consequential sanctions.

Our proposal is congruent with the last reform to the Mexican criminal system and takes into account that organized delinquency is a case that deserves a special treatment in criminal justice. Therefore, we propose that nobody but criminals be restricted to use, import, export or develop encryption. The system we suggest differentiates criminals from "organized delinquents" and other criminals who have abused encryption to further crimes. These latter cases should also involve aggravation of punishment in relation with the first condemnation. Furthermore, our proposal ensures that these people are subject to future restrictions, which should be defined by the Committee. This is the only case where escrow restrictions are not only justified, but necessary.

Legislative proposal on lawful compulsory decryption on criminal cases.

Any person within the Mexican national territory[320] shall provide the plaintext of an encrypted document -or, if it be impossible for the person under investigation to do so, by exceptional provision of a copy of the key- to the judicial authority if it so requires.

Rationale:

The parameters under which decryption is regulated can make a difference between a "law enforcement-personal freedom" balanced system and one that is not.

If a private document is encrypted and if there is a lawful cause that motivates its decryption, the document's owner must provide the contents of encrypted data, or *exceptionally* provide the key pursuant to a judicial order.

Under the terms of our suggestion, only judges are authorized to order decryption, upon request of the investigative authorities, if they decide from the petition that there are sufficient elements that justify decryption. Decrypted information should only remain in the hands of the judges, and if they decide that decrypted information is connected with the facts that motivate the investigation, they will pass that information over to the intelligence authorities. If they decide that decrypted information is not relevant to the ends of the investigation, judges should return the information to its owner, and keep what they found under strict

[320] *See* the terms of article 42 of the Mexican Constitution, *supra*, note 236, defining what the Mexican national territory comprehends.

professional secret.

The decryption judicial order should be expeditious, and in case of organized delinquency, we propose that the judges decide on it in a term of 24 hours.

Legislative proposal on key escrow.

The Mexican Government shall not adopt mandatory key escrow systems. These systems will always be optional, except in the cases defined in the legislative proposal concerning the criminal use of encryption. In the event of the emergence of an international escrow system, the Committee shall ensure that it leaves intact the rights of Mexicans before recommending its acceptance.

Rationale:

As concluded before, escrow systems implicate serious disadvantages that make them too inappropriate to be compulsory.[321] There are important constitutional objections against these systems. Therefore, we propose to exclude them as much as possible from the Mexican arena. There are some cases, however, where escrow systems may be included. For instance, official communications between governmental institutions, or between the Government and private entities, escrow is not a risk for individual privacy. The hypothetical acceptance of an international escrow system is another case where escrow should be considered. We propose that, in these cases, as well as in the case of voluntary escrow, the Committee works with the Congress to define the parameters for the use of these systems and ensure that constitutional rights remain intact.

[321] *See*: *Supra*, Chapter III, part 3, sections A) through E).

3. Conclusions.

As we have seen, it is a fact that information technologies are globally having an impact in production structures and commercialization of goods and services, and are increasingly becoming a strategic tool for countries' development.

Mexico is already part of this dramatic change and is potentially at a high risk of privacy erosion for individual, industrial and even governmental users because of the hazards that this high level of comfort unavoidably carries. Encryption may provide solutions to these concerns, but it can also represent a law enforcement concern if it is used to further crimes.

The great challenge for law today around the world is to achieve a balanced answer that ensures the greatest possible amount of privacy without conflicting with the law enforcement course. Mexican courts will have to face the challenge of resolving all the conflicts that encryption use will soon create. Among all these potential difficulties, the Mexican legal system will have to consider the debate between personal privacy and crime combat and prosecution, and it will have to provide an answer.

From the answers outlined to achieve this balance, an effective system requiring decryption is more positive than a compulsory escrow which would amount to ask citizens to organize their private communications in a way that makes hypothetical future interventions easier for the authorities. In the event of a mandatory escrow system becoming law in the future, despite today's prevailing opposition to any form of key escrow, courts would have to solve serious constitutional problems that such a system would create. They would probably base decisions, under current law, on their metaphoric identification of cryptography or the encryption key, and consequently decide how much constitutional protection the encrypted information receives. A focus on protecting the contents of information will yield higher protections (such as language, documents, possessions or even self-incrimination constitutional prohibition), while a focus on the way this information travels or is stored would yield lower protections.

The decryption system we propose for criminal cases is more appropriate because it achieves important goals. It allows expeditious access to encrypted information that is needed in an investigation, as well as privacy protection to information that is not relevant to the investigation. This system needs to be perfected yet, specially in the case of an "indicted" refusing to comply with the judicial order to decrypt his/her messages, but it is clearly more convenient than mandatory escrow.

Mexico is urged to adjust its laws to new technological developments, and to clearly define the border between privacy and national security when they conflict. Mexican law will also have to define the illegal and the beneficial uses of encryption. Society must be protected from abusive and negative uses of encryption technologies, as well as from arbitrary governmental intrusion into people's privacy.

This will require Mexican Government, the Mexican Congress and the Committee to recognize the administrative and legal dispersion that surrounds new communication technologies today, and to consolidate a comprehensive legal and administrative infrastructure. The parameters we propose include: a) a constitutional review of the constitutional doctrine on privacy and national security; b) a comprehensive regulation of encryption use in the Federal Telecommunications Act; c) a review of the criminal dispositions that pertain to abuse of encryption technologies, defining solutions to control the criminal use of encryption, in harmony with the combat against organized delinquency, and establishing the decryption system we propose; d) the abstention of treating encryption as a munition. We also support the Proposal of the Committee to create inter-secretarial commissions in order to guarantee the fulfillment of the IDP purposes.

Encryption offers important advantages to commercial, professional, and personal users of telephones, computers, and computer networks. Therefore, we also propose that the Committee actively promote the use of cryptographic technologies for protection and authentication, which will contribute to the commercial development of the country. In addition, we urge that every Mexican be able to have lawful access to use the encryption program of his/her choice, and that the Mexican Government guarantees to its citizens the right of developing, marketing, importing or exporting any encryption product. We also propose that in no event should the Mexican Government impose any compulsory encryption standard or system that implies the delivery of a copy of the citizen's private keys, except in the case of criminal use of encryption.

The purpose of the proposals is not to provide a final answer to these issues; rather, it is to initiate a discussion and to provide examples of how the parties can negotiate a solution that protects personal and commercial privacy, ensures effective law enforcement and leaves Constitutional guarantees intact.

This will not be an easy task, but it surely is one that the Committee, the Mexican Congress, and all Mexicans involved in this process will have to undertake.

4. Epilogue.

On the night of October 15th., 1996, the Mexican Senate approved the "Federal Law Against Organized Delinquency". As of October 29th., 1996, the law has not yet been ratified by the Lower Chamber and, thus, is not yet published. Under the terms of the Mexican Constitution,[322] if the Chamber of Representatives -functioning in this case as "chamber of reviewing"- does not have any comments to make on the project, the bill will go directly to the Executive for observations. If the Executive does not make any comments on the bill within 10 days, then it shall send the bill to be immediately published in the Federal Register.[323] It seems that the project will be approved quickly, since the Senate approved by the "fast-track" in a single session, adding that this bill was "urgent and of obvious solution".[324]

Unfortunately, we can not analyze the specific terms under which it will now be legal to intercept private communications.

The project, however, foresaw punishment in terms of fines and imprisonment for unlawful intervention of private communications and distribution of data, images or information obtained in such an intervention.

The project also contemplated lawful private communication intervention by mandate of the competent judicial authority, upon request of the Attorney General, in certain criminal cases (we still do not know exactly which cases, but it can be inferred that these cases should be those referred to in the last reforms to the Criminal and Criminal Proceedings Codes). This study evidences how unfruitful such interventions can be if strong cryptography is in the

[322] *See*: article 72 of the Mexican Constitution. *Supra*, note 236.

[323] *Ibid.* sections a) and b).

[324] *See*: *"Aprueba el Senado por Vía Rápida la Reforma Contra el Crimen Organizado"*. La Jornada. October 16th., 1996. Mexico City, Mexico.

hands of criminals.

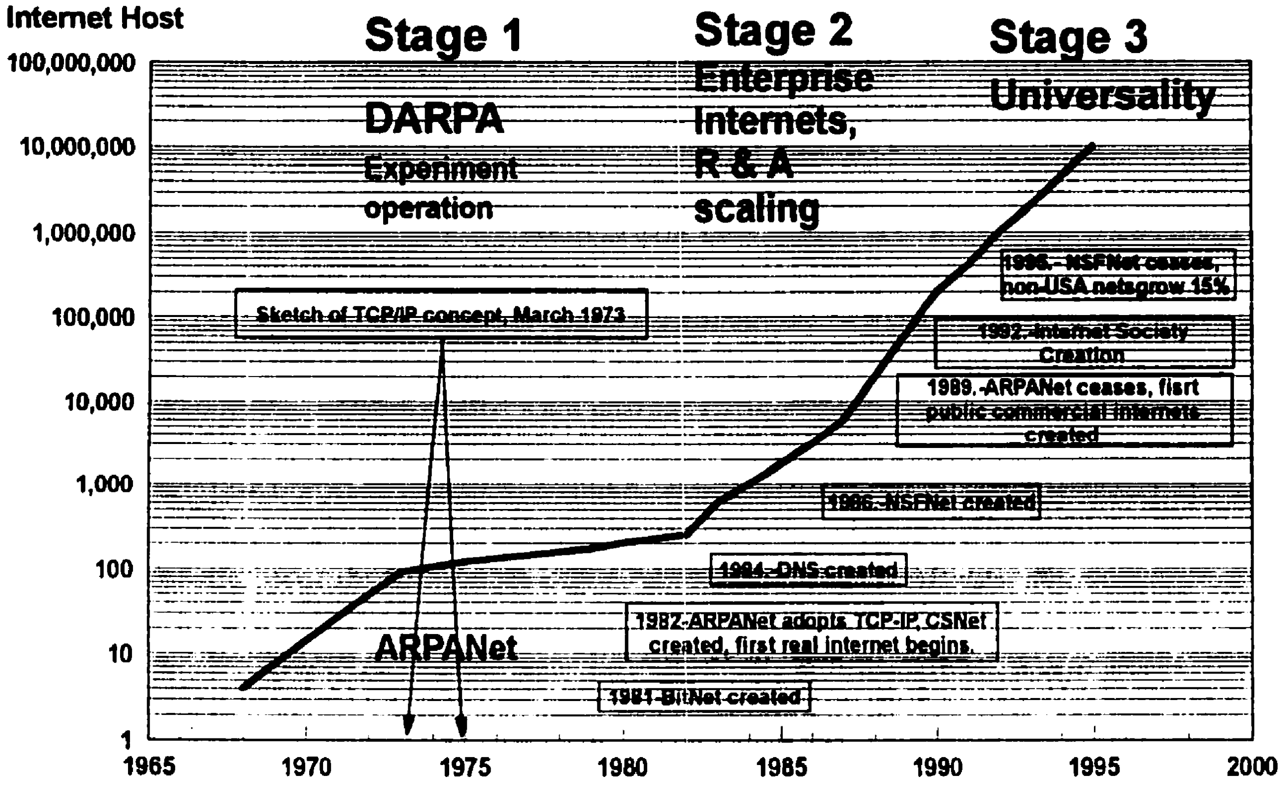
Whatever the terms of the new law are, there is something certain: regulation of encryption, personal privacy and national security are still unsolved issues. Law enforcement authorities will now have jurisdiction to intercept private communications, but this fact does not ensure the effectiveness of such measures.

Without a doubt, the debate between law enforcement and confidentiality protection has now began in Mexico. The work of the Committee will not be directed by hypothetical situations anymore, but by real facts. The need for a systematic legislative review has grown and the role of the Committee has acquired a greater new dimension.

5. Graphs.

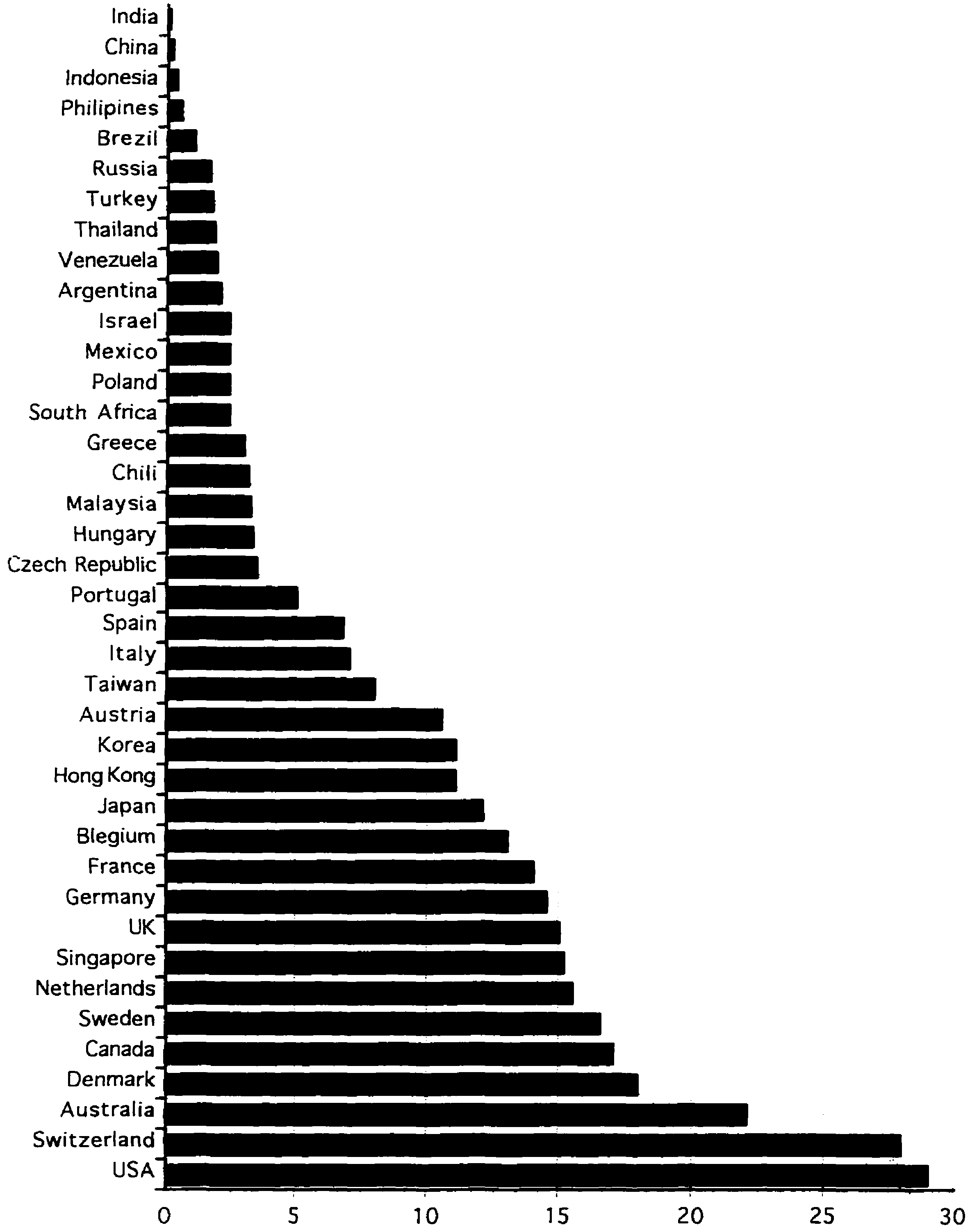
Graph No. 1

Internet Evolution



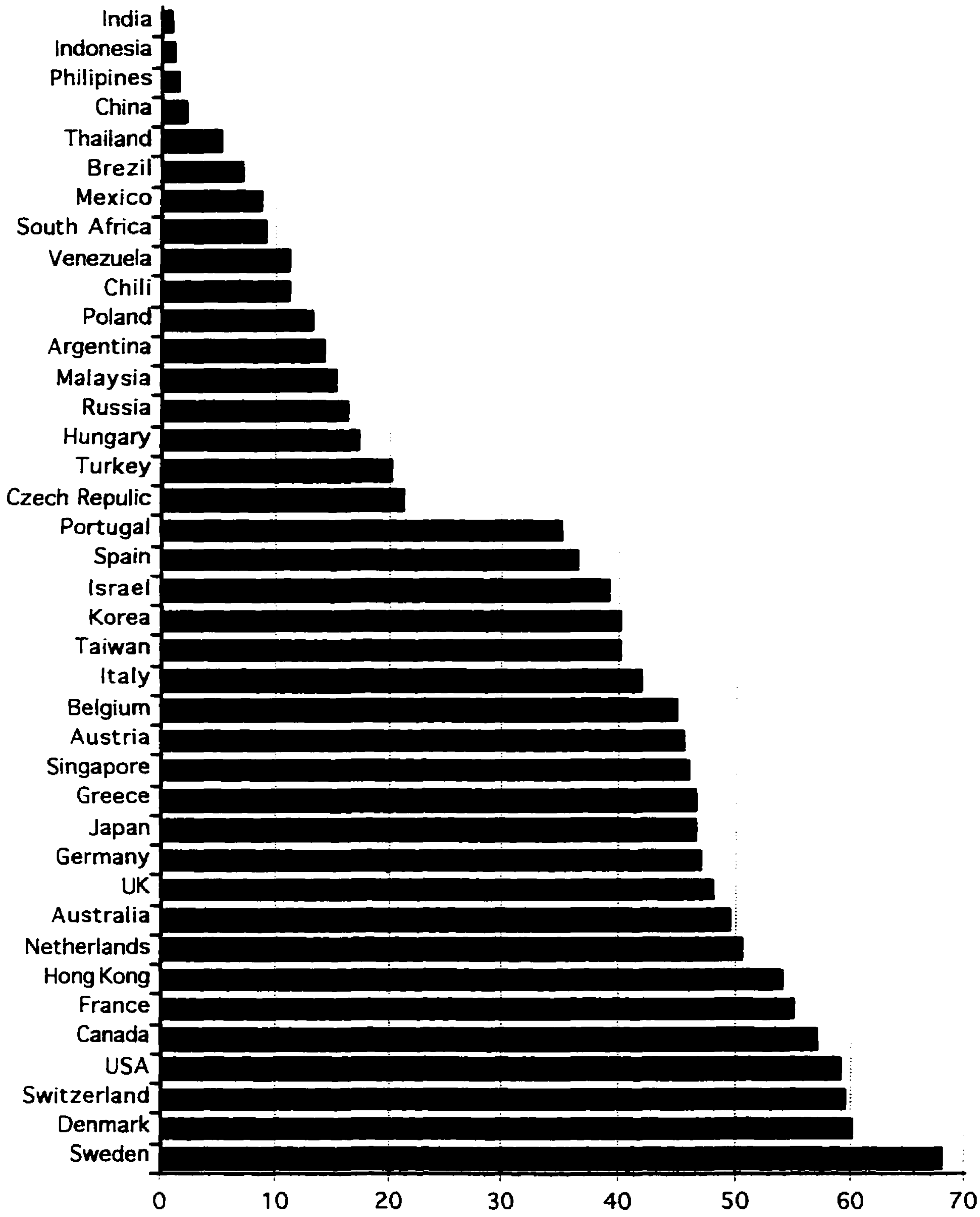
Source: URL http://www.nic.mx/NIC/IMAGES/ISOC/timeline.gif

GRAPH No. 2. PCs Density
(per 100 inhabitants)



Source: International Telecommunications Union,1995, cited by INEGI, Computational modulus. Informatic Development Program. Available online at URL: http://inegi.gob.mx/homepara/pdi/pdi/pag4.html.

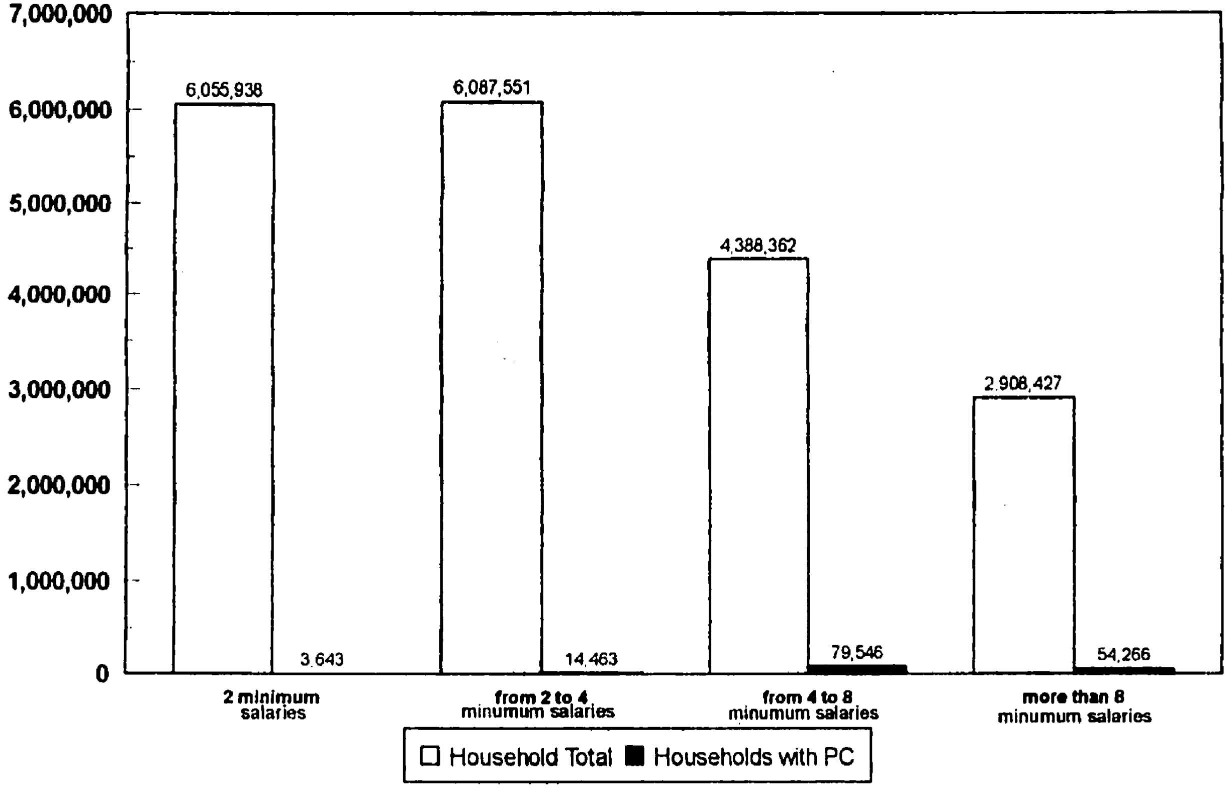
GRAPH No. 3. Telephonic density
(per 100 inhabitants)



Source: International Telecommunications Union, 1995, cited by INEGI, Computational modulus, Informatic Development Program. Available online at URL: http://inegi.gob.mx/homepara/pdi/pdi/ pag19.html.

Graph No. 4

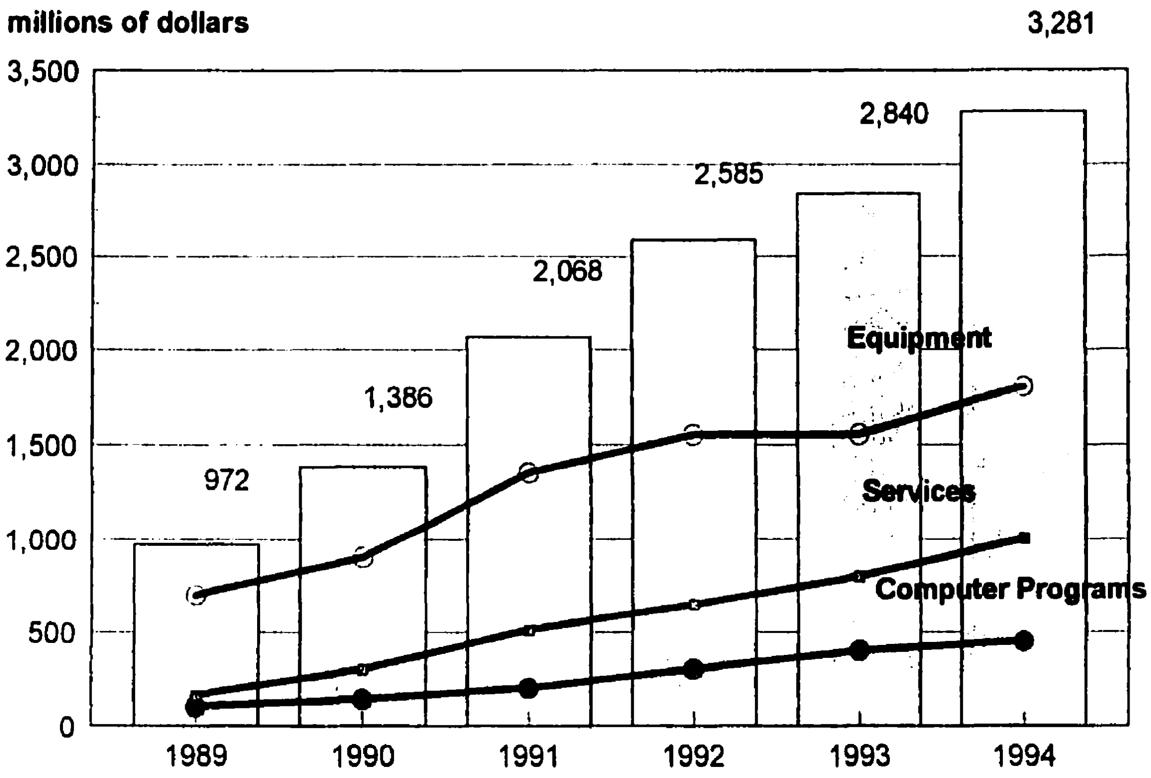
Households with PC in relation with total household per income average



Source: INEGI-ENIGH, 1994, available at: URL http://www.inegi.gob.mx/homepara/pdi/pdi/pag8.html

Graph No. 5

Informatic Products Demand in Mexico



Source: International Data Corporation-SELECT, available on line at: URL
http://www.inegi.gob.mx/homepara/pdi/pdi/pag18.html

BIBLIOGRAPHY.

GOVERNMENT DOCUMENTS AND LEGISLATION:

- *Amendment to the US's International Traffic in Arms Regulations.* Federal Register Vol. 61, No. 33. Rules and Regulations. Department of State, 22 CFR Parts 123 and 126. February 16th., 1996. Available online at URL: http://www.law. Miami.edu/~froomkin/ persuse.htm.

- California Government Code. S 16.5 (Enacted Oct. 4, 1995).

- Criminal Code for Mexico City in Common Jurisdiction, and for the entire Republic in Federal Jurisdiction ("*Código Penal Para el Distrito Federal en Materia del Fuero Común y para toda la República en Materia del Fuero Federal*"), published in the Federal Register ("*Diario Oficial de la Federación*") on August 14th, 1931. Mexico.

- "*Elements for Strategic Programs on Informatic Policies.*" Consultant Committee on Informatic Policies. National Institute of Statistics, Geography and Informatics. Mexico. October, 1994, at 39. Available on-line at URL: http://inegi.gob.mx /homepara/pdi/.

- Federal Act of Fire Arms and Explosives ("*Ley Federal de Armas de Fuego y Explosivos*"), published in the Federal Register ("*Diario Oficial de la Federación*") on Jan. 11th., 1972.

- Federal Act of Fire Arms and Explosives' Regulations ("*Reglamento de la Ley Federal de Armas de Fuego y Explosivos*"), published in the Federal Register ("*Diario Oficial de la Federación*") on May 6th., 1972.

- Federal Code of Criminal Procedures *("Código Federal de*

Procedimientos Penales"). Published in the Federal Register *("Diario Oficial de la Federación")*, on November 17th, 1931. Mexico.

- Federal Public Administration Act. (*"Ley Orgánica de la Administración Pública Federal."*) Published in the Federal Register ("*Diario Oficial de la Federación*") on December 29th., 1976.

- Federal Telecommunications Act. (*Ley Federal de Telecomunicaciones*). Published in the Federal Register (*Diario Oficial de la Federación*) on June 7th., 1995. Mexico.

- General Communications Channels Act (*"Ley de Vías Generales de Comunicación*"), published in the Federal Register on February 19th., 1940.

- *Meeting to introduce the Informatic Development Program 1995-2000*, April 12, 1996. Presentation speech by Dr. C. M. Jarque, Chairman of the National Institute of Statistics, Geography and Informatics (Mexico City, National Institute of Statistics, Geography and Informatics). Available online at URL: http://inegi.gob.mx/homepara/pdi/.

- Mexican Foreign Service Act's Rules ("*Reglamento de la Ley del Servicio Exterior Mexicano"*). published in the Federal Register (*Diario Oficial de la Federación*) on October 11th., 1994.

- Mexico's National Development Plan (*"Plan Nacional de Desarrollo"*) 1995-2000. Office of the President of the United Mexican States. May 8th., 1995. Available online at URL: http://www.inegi.gob.mx/homepara/pdi/

- Mexico's Statistic and Geographic Information Act (*"Ley de Información Estadística y Geográfica*") published in the Federal Register on December 30th., 1980.

- Minister of Supply and Services. *Access, Affordability and Universal Service on the Canadian Information Highway.* Information Highway Advisory Council. Canada, January 1995.

- Minister of Supply and Services. *Connection Community Content. The Challenge of the information Highway.* (Canada: Final Report of the Information Highway Advisory Council, September 1995).

- Minister of Supply and Services. *The Canadian Information Highway: Building Canada's Information and Communications Infrastructure.* Information Highway Advisory Council, Industry Canada, April 1994.

- Minister of Supply and Services. *Privacy and the Canadian Information Highway: Building Canada's Information and Communications Infrastructure.* (Canada: Industry Canada, October 1994).

- Minister of Supply and Services. *Canada's Information Highway: Building Canada's Information and Communications Infrastructure. Providing New Dimensions for Learning, Creativity and Entrepreneurship.* Progress report of the Information Highway Advisory Council, Canada, November 1994.

- Political Constitution of the Mexican United States, ("*Constitución Política de los Estados Unidos Mexicanos*"), Published on February 5th., 1917. Editorial Porrúa. Mexico, 1992, at article 10.

- USA's Arms Export Control Act, codified as amended at 22 USC. Sec. 2778 (1988 & Supp. IV 1992).

- USA's Encrypted Communications Privacy Act. S.1587. s. 104th Cong. Sess. (1996.)

- USA's Export Administration Act of 1979, as amended by the Export Administration Amendments Act of 1985 (50 USC. App. 2401-2420) and the EAR (15 C.F.R. ss. 768-799).

- USA's International Traffic in Arms Regulations. 22 C.F.R. Parts 120 *et seq.* (1994).

- USA's Promotion of Commerce Online in the Digital Era Bill.

S. 1726 is 104th. Congress 2nd. Session, May 2nd., 1996.

- USA's Security And Freedom through Encryption Act. HR 3011. 104th Cong. 2nd Sess. (1996).

- *US Administration Statement on Commercial Encryption Policy*. Executive Office of the President, Washington, D.C. (July 12th., 1996). Available online at URL http://csrc.hcsl.nist.gov/keyescrow/admin.txt.

- US Department of Commerce and the National Security Agency. *A Study Of The International Market For Computer Software With Encryption*. Document prepared for the Interagency Working Group on Encryption and Telecommunications Policy. Available online at: URL ftp://ftp. cygnus.com/pub/export/.

- US Department of Justice, *"Attorney General Makes Key Escrow Encryption Announcements"* 2 (February 4th., 1994), *in:* Office of the Press Secretary, The White House, *"Key Escrow Encryption: Announcements"* (February 15, 1994.)

- Utah Code Ann. S. 46-3-101 *et seq.* (eff. May 1, 1995)

CASES, MEXICAN JURISPRUDENCE AND COURTS' CRITERIA:

- Bernstein v. United States Department of State (Civil Action No. C9500582-MHP N.D. Cal. 1996). Available online at URL: http://www.eff.org/pub/Privacy/ITAR_export/Bernsteincase/Legal/960415.decision.

- Case #1:95CV01812 in the DC Federal District Court. September 21st., 1995.

- Commodity Jurisdiction Case 038-94.

- Commodity Jurisdiction Case 081-94.

- Karn v. United States Department of State (D.C. Cir. 1996), available online at URL http://www.qualcomm.com/people/pkarn/export/decision.html960415.decision.

- People of the State of New York v. Leary, Part 72. January 8, 1996. (NY. App. Div. 1996).

- *"Semanario Judicial de la Federación." "Amparo administrativo en revisión"* 367/ 32, September 25th., 1933, unanimity of 4 votes. Reg. 586, year 1933, epoch 5, t. XXXIX.

- *Ibid. "Amparo administrativo en revisión"* 5377/44, April 20th., 1945, unanimity of 4 votes. Reg. 589, year 1945, epoch 5. T. LXXXIV, p. 910.

- *Ibid. "Amparo Civil en Revisión"* 402/40. Unanimity of 4 votes. July 24th., 1941. Reg. 905, year 1941, epoch 5, t. LXIX, at 1329.

- *Ibid. "Amparo Civil en revisión"* 5779/38. March 21st., 1941, unanimity of 5 votes. Reg. 792, year 1941, epoch 5.

- *Ibid. "Amparo directo"* 44/90. November 14th., de 1990. Unanimity of votes. Reg. 6010, year 91, epoch 8.

- *Ibid. "Amparo directo"* 539/92. Reg. 8426, year 1993, epoch 8. January, 1993. Unanimity of votes.

- *Ibid. "Amparo directo"* 633/89. May 23rd., 1989. Majority of votes. Reg. 5078, year 89, epoch 8.

- *Ibid. "Amparo en revisión"* 59/91. Reg. 5769, year: 91, epoch: 8. April 30th., 1991, unanimity of votes.

- *Ibid. "Amparo en revisión"* 212/90. Reg. 5736, year 91, epoch 8. June 28th., 1990. Unanimity of votes.

- *Ibid.* "*Amparo en revisión.*" 236/93, September 2nd., 1993, unanimity of votes. Reg. 8639, year 1993, epoch 8.

- *Ibid.* "*Amparo en revisión*" 508/89. July 4th., 1991. Unanimity of votes. Reg. 5815, year 91, epoch 8.

- *Ibid.* "*Amparo en revisión*" 704/88. March 10th., 1989. Unanimity of votes. Reg. 5478 year 89, epoch 8.

- *Ibid.* "*Amparo en revisión*" 791/80. March 25th., 1981. Reg. 915, year 1981, epoch 7. Vols. 145-150, 6th. part, unanimity of votes.

- *Ibid.* "*Amparo en revisión*" 1041/81, April 16th., 1982, majority of votes. Reg. 918, year 1982, epoch 7, Inform 1982, 3rd. part.

- *Ibid.* "*Amparo en revisión*" 1389/71. September 4th., 1975, 5 votes.

- *Ibid.* "*Amparo en revisión*" 5097/58, January 30th., 1961, majority of 3 votes. Reg. 770, year 1961, epoch 6, Vol. XLIII, 3rd. part.

- *Ibid.* "*Amparo en revisión*" 7005/65. Reg. 844, year 1968, epoch 6, vol. CXXVIII, 3rd. part.

- *Ibid.* "*Amparo penal directo*" 8437/37, April 20th., 1938, unanimity of 4 votes. T. LVI, p. 629. Reg. 1101, year 1938, epoch 5.

- *Ibid.* "*Amparo penal directo*" 11443/32, September 11th., 1934, majority of 4 votes. T. XLII, Reg. 480, year 1934, epoch 5.

- *Ibid.* "*Amparo penal en revisión*", Reg. 221, year 1918, epoch 5, t. II, at 395. February 8th., 1918, majority of 6 votes.

- *Ibid.* "*Amparo Penal en revisión.*" Reg. 407, year 1920, epoch 5, t. vii, at 1120. Majority of votes.

- *Ibid.* "*Amparo penal en revisión*" 3941/37. Reg.. 620 & 895, Year: 1937, Epoch: 5, T. LIII, p. 2568. September 3rd., 1937, unanimity of 5 votes.

- *Ibid.* "*Amparo penal en revisión*" 11290/32, February 8th., 1934, unanimity of 5 votes. Reg. 215, year 1934, epoch 5, t. XL, at 1275.

- *Ibid.* Mexican Jurisprudence Thesis number 6/1993. Mexico, City. October 8th., 1993. [Antecedents: 1.- "*Amparo en revisión*" 1111/92. July 1st., 1993, majority of 17 votes. 2.- "*Amparo en revisión*" 247/93 July 10th., 1993, majority of 17 votes. 3.- "*Amparo en revisión*" 367/93. July 1Oth., 1993, majority of 17 votes. 4.- "*Amparo en revisión*" 587/93, July 10th., 1993, majority of 15 votes. 5.- "*Amparo en revisión*" 1167/92, August 3rd., 1993, majority of 16 votes.]

- *Ibid.* Reg. 489, year 1975, epoch 0, Vol. 81, 3rd. part Reg. 2450, year 1924, epoch 5, t. XIV, p. 286, January 17th., 1924, unanimity of 8 votes.

- *Ibid.* Reg. 635, year 1919, epoch 5, t. IV, at 1119. June 6th., 1919. Unanimity of 11 votes.

- *Ibid.* Reg. 638, year 1918, epoch 5, t. III, November 4th., 1918. Unanimity of 8 votes.

- *Ibid.* Reg. 904, year 1929, epoch 5, T. XXV. February 29th., 1929. Unanimity of 5 votes.

- *Ibid.* Reg. 6814, year 90, epoch 8, "*Amparo en revisión*" 250/39. March 30th., 1990. Unanimity of votes.

- *Ibid.* Reg. 8127, year 1993, epoch 8. Thesis no. X/93, January 12th., 1993.

- *Ibid.* "*Revisión principal*" no. 425/87, reg. 6348, year 88, epoch 8. September 29th., 1988. Unanimity of votes.

BOOKS:

- I. Burgoa Orihuela. "*Las Garantías Individuales.*" Editorial Porrúa. 26th., edition. Mexico, 1994.

- Cheswick, W. R. and Bellovin, S. M. "*Firewalls and Internet Security: Repelling the Wily Hacker.* Addison-Wesley Professional Computing Series. Massachusetts, April, 1995.

- L. J. Hoffmann, ed. *Building In Big Brother: The Cryptographic Policy Debate.* Springer Verlag. March, 1995.

- D. L. Johnston, D. Johnston & S. Handa. *Getting Canada On Line: Understanding the Information Highway.* (Toronto: Stoddart Publishing, 1995).

- Levine, John R. and Baroudi, Carol. *Internet Secrets.* IDG Books Worldwide. US, 1995.

- L. Rose. *Netlaw: Your Rights in the Online World.* Osborne McGraw Hill. US 1995. 372 pp.

- Schneier, B. *Applied cryptography* , John Wiley & Sons, (US, 1994).

- T. J. Smedinghoff, Ed. *Online Law: The SPA's Legal Guide to Doing Business on the Internet.* (Massachusetts: Addison-Wesley, 1996.)

- Stallings, William. *Networking and Inter-network Security: Principles and Practice.* Prentice-Hall. (New Jersey, US 1995.)

- P. R. Zimmermann. *The official PGP User's Guide.* (Cambridge, Massachusetts, MIT Press. 1995). 127 pp. Available online URL fttp://net-dist.mit.edu/pub/PGP/

JOURNALS AND PERIODICALS:

- Abramson, Ronald. *"Protecting Privilege in E-mail systems"*, Legal Times, Aug. 15, 1994

- *"Aprobarla Sería una Flagrante Violación a la Constitución."* La Jornada. November 15th., 1995, Mexico City, Mexico.

- "*Aprueba el Senado por Vía Rápida la Reforma Contra el Crimen Organizado.*" La Jornada. October 16th., 1996. Mexico City, Mexico.

- S. A. Baker. *"Don't Worry, Be Happy: Why Clipper Is Good For You,"* [June 1994] Wired.

- Barrister, Ed. *"Who Has the Right of Way? Intellectual Property Rights on the Internet."* (1996) 22, Barrister Magazine. No. 4, at 25-29.

- J. P. Chandler *"Identification and Analysis of Foreign Laws Pertaining the Use of Commercial Encryption Products."* (Washington, National Intellectual Property Law Institute and George Washington University. Jan., 1994). Available online at URL: http://www.sevenlocks. com/papers/crypto/lawfor. txt.

- M. M. Cleh, *"Government Control of Private Ideas-Striking a balance Between Scientific Freedom and National Security."* (1982) Jurimetrics Journal. No. 1, 22.

- J. Erickson, "*Cryptology Fires Up the Feds*", [1993] Dr. Dobb's Journal, 6.

- M. A. Froomkin, "*The Metaphor is the Key: Cryptography, the Clipper Chip and the Constitution.*" 143 U. Pa. L. Rev. n3, 707-807.

- G. Garon & R. Outerbridge, *"DES Watch: An Examination of the Sufficiency of the Data Encryption Standard for Financial*

Institution Information Security in the 1990's", [July 1991] Cryptologia.

- Hardley, T. "*The Proper Legal Regime of Cyberspace.*" University of Pittsburgh Law Review. (Summer, 1994) Vol. 55, p. 993-1055.

- Heels, E. and Klau, R. P. "*Let's Make a Few Things Perfectly Clear: Cyberspace, the Internet and the Superhighway.*" Student Lawyer. May, 1995, p. 15-17.

- L. J. Hoffmann *et al.* "*Cryptographic Policy*", (Comm. ACM, Sept. 1994.)

- J. L. Kashi, "*Protecting Client Confidences in the Electronic Age.*" [1995] Law Practice Management, at.

- Katsh, Ethan. "*Law in a Digital World: Computer Networks and Cyberspace.*" Villanova Law Review. April, 1993, Vol. 38, p. 403-455.

- R. P. Klau & J. Heels, "*There is still not a single comprehensive resource for learning about the law that relates to the Internet.*" Student Lawyer. November 1995, at 12.

- S. Landau, *et al.* "*Codes, Keys and Conflicts: Issues in US Crypto Policy.*" Discrete Mathematics Seminar. Rutgers University. February 16th., 1995.

- S. Levy, "*The NSA is Not Alone*", Wired 1. February, 1993. Available online at: URL http://www.hotwired.com/wired/1.2/features /crypto.rebels.sidebars.htm#nsa-not-alone.

- J. Markoff, "*Federal Inquiry on Software Examines Privacy Programs,*" New York Times, 21 September 1993, C1.

- G. Murphy. "*Directive: Electronic Funds and Securities Transfer Policy-Message Authentication and Enhanced Security.*" US Department of the Treasury. No. 16-02 s. 03 (Dec. 21, 1992.)

- "*PGR: Se Prepara una Iniciativa para Reglamentar el Espionaje Telefónico.*" La Jornada, May 24th., 1995. Mexico City, Mexico.

- Plascencia Villanueva, Raúl. "*La Reforma al Código Penal Para el Distrito Federal en Materia del Fuero Común y para toda la República en Materia del Fuero Federal.*" Available on-line URL http://info.juridicas.unam. mx:80/infojus/

- "*Power vs. Informatic Privacy: Debate Zimmermann-Kallstrom.*" *La Jornada en Internet*, Virtualia Review no. 2, February 26th., 1996, available online at URL: http://serpiente.dgsca.unam. mx/Jornada.

- "*Puentear líneas para Gobernación, orden de rutina en Telmex.*" La Jornada, May 26th., 1995. Mexico City, Mexico.

- E. J. Radlo. "*Legal issues in cryptography.*" (US: Fenwick & West. Jan., 1996.)

- "*Reunión de Procuradores y Ombudsman.*" La Jornada, April 29th., 1996. Mexico City, Mexico, at 8.

ONLINE SOURCES:

- B. Aboba. *"How the Internet Came to Be"*, in *"The Online User's Encyclopedia"* (1993), available online URL gopher:// gopher.isoc.org:70/00/Internet/ history/how.internet.came.to.be.

- "*Alert from a coalition of online civil liberties organizations.*" August 7th., 1996. Available online at: URL http://www. aclu.org/gilc/index1.html.

- Anonymous. *"Encryption: A Free Society's Dilemma: A Discussion of Legislative Proposals to Regulate the Use and Export of*

Encryption Technology.." Available online at URL http://www.law.miami.edu/~froomkin/seminar/papers/anon/ intlaw-paper.html.

- S. A. Baker, "*Emerging Japanese Encryption Policy.*" Available online at URL: http://www.usnet/~steptoe/276915.htm.

- S. A. Baker, "*Summary of the OECD Meeting of Experts on Cryptography.*" Organization for Economic Cooperation and Development. Available online at: URL: http://www.us.net/~Steptoe/276908.html.

- M. S. Baum. "*Digital Signature Primer in Verisign, Inc.*" Frequently Asked Questions Appendix 1 (June 23rd., 1995). Available online at URL http://www.verisign.com/faq.

- M. Blaze *et al.* "*Minimal Key Lengths For Symmetric Ciphers To Provide Adequate Commercial Security.*" Jan., 1996. Available online at URL http://www.bsa.org/bsa/cryptologists. html.

- E. F. Brickell *et al.* "*SKIPJACK Review Interim Report: The SKIPJACK algorithm.*" (July 28th., 1993). Available online at URL http://www.quadralay.com/www/crypt/clipper/Skipjack-review. html.

- Bortzmeyer, S. "*L'utilisation du chiffrement en France.*" Gopher://gopher.urec.fr/00/securite/ docs/lois/dssi_scssi. txt.

- C. Burns. "*Open Letter to Internet Community From Senator Burns.*" May 2nd., 1996. Available online at URL http://www.privacy.org/ipc/#resources/burns/.

- C. Burns. "*Press announcement of the Pro-CODE: Burns Has 'CODE' for E-Commerce: Legislation Opens Internet for Commerce, Protects Intellectual Property.*" Available online at URL http://www.privacy.org/ ipc/#resources/burns/.

- V. Cerf, "*A Brief History of the Internet and Related Networks*", available online at: URL gopher://gopher.isoc.org:70/00/Internet/history/_A Brief History of the Internet and Related Networks_ by V. Cerf.

- Committee to Study National Cryptography Policy. "*Cryptography's Role in Securing the Information Society. Overview and Recommendations.*" (Computer Science and Telecommunications Board; National Research Council; National Academy of Sciences and National Academy of Engineering.) May 30, 1996. Available online at: URL http://www.lotus. com/notesr4/crypt-or.htm.

- "*Current controversy surrounding RSA.*" Available online at URL: http://www.library.carlton.edu/student-workers/dan/rsa. html.

- D. Denning, "*Letter to Senator Patrick Leahy.*" March 14th., 1996. Available Online URL http://www.cdt.org/crypto/.

- D. Denning, "*The Future of Cryptography.*" Available online at: URL http://www.eff.org/pub/Crypto/ITAR_export/Key_escrow/ denning_0.

- P. Fahn. "*Frequently Asked Questions About Today's Cryptography*", (May 5th., 1995), available online at: URL ftp://pub /usenet/news.answers/ cryptography-faq/RSA/

- Files on the Karn case, available at URL http://www.qualcomm.com/ people/pkarn/export/.

- "*The Free On-Line Dictionary of Computing*", available online at: URL http://wombat.doc.ic.ac.uk/?World-Wide+Web.

- "*ITAR Export Restrictions.*" Available online at URL http://www.eff.org/pub/crypto/ITAR/export/. Also: *Privacy - Crypto - ITAR Export Restrictions Archive*, available online at URL http://www.eff.org/pub/Privacy/ ITAR_export/.

- Leahy, P. "*Statement of Senator Patrick Leahy on Introduction of Encrypted Communications Privacy Act of 1996.*" March 5th., 1996. Available online at URL http://www.cdt.org/crypto/leahy_ statement.html.

- "*La loi sur les télécoms met l'Internet en laisse.*" Bulletin lambda 2.08. June 10th., 1996. Available online at URL http://

www.freenix.fr/netizen/208. html.

- B. W. McConnell, E. J. Appel & Co-Chairs, Interagency Working Group on Cryptography Policy. *"Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure."* Executive Office of the President, Office of Management and Budget, Washington, D.C. May 20, 1996 Available online at URL: http://www.isse.gmu.edu/~pfarrell/NIST/kmi.html.

- S. McLandish, responding to Dorothy Denning's *The Future of Cryptography*, available online at http://www.eff.org/pub/Crypto/ITAR_export/Key_escrow/denning_02.

- Pro-CODE and ECPA texts available online at: URL http://www.cdt.org/crypto/or http://thomas.loc.gov.

- P. R. Reitinger, "*Compelled Production of Plaintext and Keys*", January 16, 1996. Available online URL "http://law.lib.uchicago.edu/forum/reitinger.html.

- "*Relatoria del Primer Evento del Foro de Consulta sobre Derecho e Informática.*" Available at URL http://www.inegi.gob.mx/homepara/pdi/pdi/rela1.html.

- "*Relatoria del Segundo Evento del Foro de Consulta sobre Derecho e Informática.*" Available at URL http://www.inegi.gob.mx/homepara/pdi/pdi/rela2. html.

- "*Relatoria del Tercer Evento del Foro de Consulta sobre Derecho e Informática.*" Available at URL http://www.inegi.gob.mx/homepara/pdi/pdi/rela3. html.

- J. Rosenoer. "*Coded Speech.*" Available online at: URL http://www.cyberlaw.com/cylw0396.html. Other files on the Bernstein case are available at URL http://www.eff.org/pub/privacy/ITAR_export/bernstein_ case/.

- "*RSA's Data Security Conference,* Remarks prepared by R. Ozzie," available online at URL http://www.lotus.com/notesr4/

ozzie.htm. January, 1996.

- B. Simons and J. B. Snyder, “*Letter to Senator Burns, supporting the Pro-CODE,*” April 2nd., 1996. Available online at URL http://www. privacy.org/ipc/#resources/burns/.

- Steptoe & Johnson LLP. “*France's Proposed Statutory Trusted Third Party Rules for Encryption.*” Available online at http://www.us.net/~steptoe/france.htm.

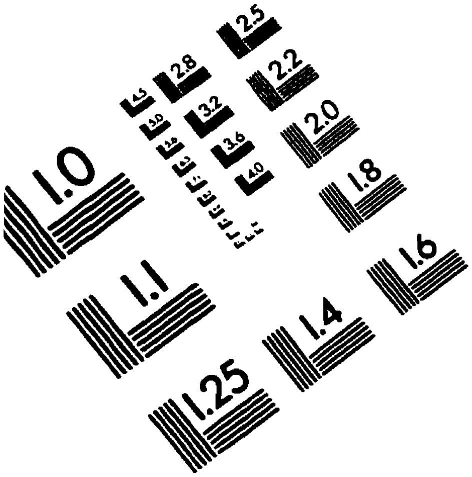
- Steptoe & Johnson LLP. “*Russian Statutes Restricting Use of Encryption Technologies.*” Available online at: http://www.us. net/~steptoe/cyber.htm

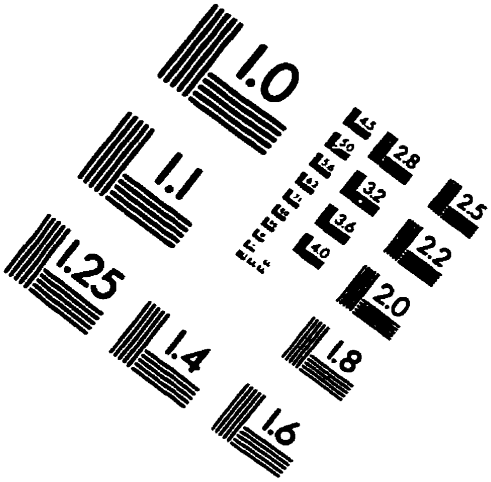
- “*Summon for the Forum on Informatics and the Law.*” August 9th., 1996. Congress of the United Mexican States. Available online at URL: http://www.inegi.gob.mx/homepara/pdi/.

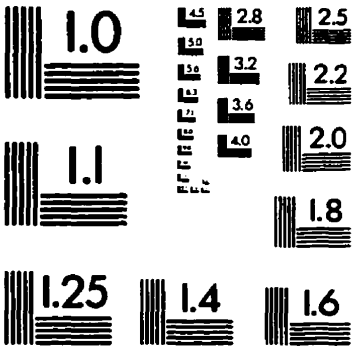
- User estimates, available at: URL http://www.commerce. net and also at: URL http://home.netscape.home/newsref/pr/ newsrelease69. html.

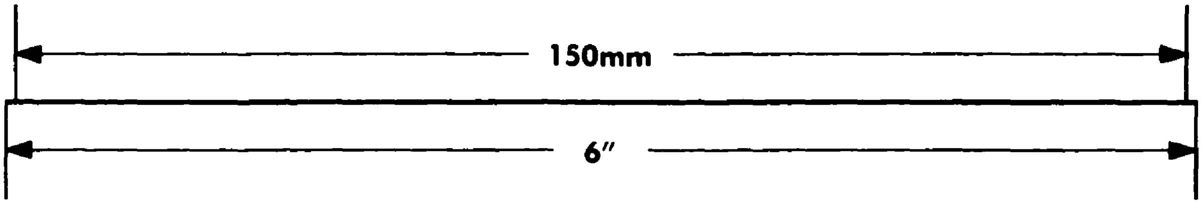
- M. Voorhees. “*A Tale of Two Crypto Court Cases Are Karn and Bernstein judges on the same planet?*” May 3rd., 1996. Available online at: URL http://www.infolawalert.com/stories/ 050396b.html.

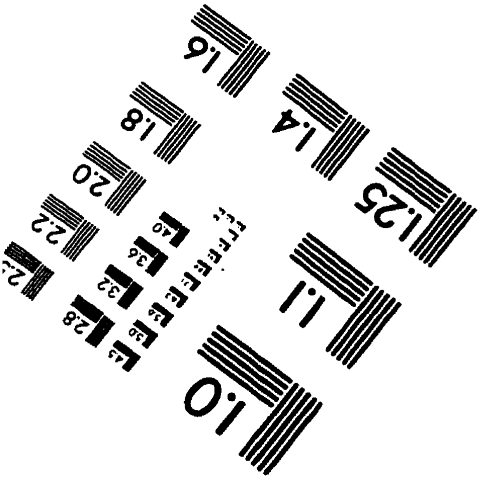
IMAGE EVALUATION TEST TARGET (QA-3)

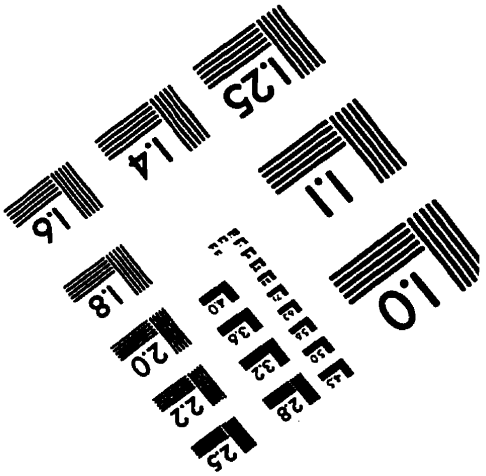












APPLIED IMAGE . Inc
1653 East Main Street
Rochester, NY 14609 USA
Phone: 716/482-0300
Fax: 716/288-5989