INFORMATION TO USERS

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

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

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

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

ProQuest Information and Learning
300 North Zeeb Road, Ann Arbor, MI 48106-1346 USA
800-521-0600

The OECD Cryptography Policy Guidelines and their implementation

Ars ipsi secreta magistro

Jean Robert du Carlet, 1644

Jonas Jeppsson
Institute of Comparative Law
McGill University, Montreal
August 2000

A thesis submitted to the Faculty of Graduate Studies and Research in partial fulfillment of the degree of Master of Laws

DEDICATION

This thesis is dedicated to my dear parents who have always supported me. Moreover, it is dedicated to my brother's four children who are a source of energy and joy for me.

Kaj and Ulla
Mats, Tina
&
Anna, Siri John and Lova

ACKNOWLEDGEMENTS

This thesis is the culmination of a long process that has opened up my eyes to a new and exciting area of law and technology. I hope that the work has brought me closer to Oscar Wilde's first category than the second.

There are only two kinds of people who are really fascinating—people who know absolutely everything, and people who know absolutely nothing.
Oscar Wilde (1854–1900), Lord Henry, in The Picture of Dorian Gray, ch. 7 (1891).

I have several persons to which I am grateful and to whom I wish to express my sincere thanks.
First of all I want to thank my supervisor Professor H.P. Glenn for encouraging comments and help. Moreover, I want to thank my dear friends and colleagues Diana and Felix for valuable comments and Yushan Ng for proof reading the thesis. As a Wallenberg scholarship holder I also want to express my sincere gratitude to Knut and Alice Wallenberg's Foundation for giving me this possibility. I, furthermore, want to thank all my friends and colleagues for a nice and stimulating time in Montreal. I will miss you all.

Those insightful words by the German philosopher Arthur Schopenhauer summarize to a great extent the work with the thesis in Montreal.

As the biggest library if it is in disorder is not as useful as a small but well-arranged one, so you may accumulate a vast amount of knowledge but it will be of far less value to you than a much smaller amount if you have not thought it over for yourself.
Parerga and Paralipomena, vol. 2, ch. 22, sct. 257 (1851).

ABSTRACTS

Abstract

The Organization for Economic Co-operation and Development (OECD) issued on 27 March 1997 a recommendation concerning cryptography policy guidelines in an attempt to foster international co-operation and harmonization. Information is becoming increasingly valuable in society. Globalization of markets, improvements in information and communication technology and the shift to a knowledge-based economy has, furthermore, created an enormous potential for electronic commerce. Conservative estimates predict electronic commerce will have a turnover of more than US $400 billion by 2002. The increasing importance of information and communications has, however, made the information society vulnerable. Cryptography plays an important part in securing transactions in electronic commerce and moreover, in establishing a secure electronic environment in the information society. Fear of privacy infringements and lack of secure methods for electronic transactions has until now been holding electronic commerce back. Cryptographic methods are an essential part in securing electronic commerce. Law enforcement agencies and national security organizations fear, however, that widespread use of strong encryption will impede their work substantially. This thesis analyzes the advantages and disadvantages of strong encryption and how the balance of the conflicting interests has been dealt with in the OECD Cryptography Policy Guidelines. Moreover, shows the thesis how the OECD Cryptography Policy Guidelines have been implemented and makes suggestions on how the guidelines should be implemented.

Introduction

L'organisation de coopération et de développement économique"(O.C.D.E.) a adopté une recommandation le 27 mars 1997, qui énonce les lignes directrices qui règlementeront la cryptographie dans le cadre d'un développement de la coopération et de l'harmonisation internationale.
Dans notre société, l'information est devenue une valeur appréciable. La globalisation des marchés, l'amélioration de la technologie de l'information et de la communication, et l'évolution vers une économie fondée sur la connaissance, ont engendré un énorme potentiel pour le commerce de l'électronique. Les estimations les plus prudentes prédisent que ce commerce représentera un chiffre d'affaire de plus de 400 milliards de dollars américains en l'an 2002. Pourtant, l'importance croissante de l'information et de la communication a rendu l'information vulnérable. C'est à ce niveau que la cryptographie joue une place importante. Elle permet la sécurité des échanges faîte par le commerce électronique, et de manière globale, la sécurité de l'environnement électronique de notre société de l'information. Elle balaye les freins de développement d'hier qui étaient la peur de la violation de la vie privée et l'absence de systèmes sûrs garantissant les transactions. Les méthodes de cryptographie constituent un point vital, même si les organes d'execution et les organisations nationales de sécurité y voient une gêne substanielle dans leur travail dans son utilisation à grande échelle.
Cette thèse porte sur les avantages et les inconvénients d'une utilisation à grande échelle de la cryptographie. Elle cherchera à montrer comment le projet de l'OCDE a trouvé un équilibre entre les différents intérêts conflictuels qui existaient. Puis, elle montrera comment ce projet pourra s'insérer dans l'utilisation déjà faîte de la cryptographie.

TABLE OF CONTENTS

Introduction

In 1995 a fierce debate raged in the USA over what very few persons until then had heard about - cryptography. Cryptography is the science of codes.[1] It is a method of encoding and decoding information by using a mathematical algorithm which can make a message unreadable for anyone else but the key holder. The US Government wanted to stop widespread use of cryptography and introduced a tamper-proof chip, in which a cryptographic algorithm was embedded, the Clipper chip. It was this chip which sparked the debate.[2] On one side privacy advocates argued that Orwell's 1984 had arrived and on the flip side representatives for the government defended the chip by pointing out that the availability of strong cryptography would render society toothless against paedophiles, drug-traffickers and terrorists. Cryptography can be used for both legitimate and illegitimate purposes and it is my firm belief that cryptography can, should, and will play an important part in the information society. I, furthermore, consider that the public debate has become too polarized - either cryptography is good or bad. Some of the arguments used in the debate have not sounded very convincing and it is my belief that one of the main reasons why governments try to restrict the use of strong cryptography is their fear of losing intelligence capability. Cryptography is interesting because it touches many areas and any related standard has to be internationally accepted. It is, however a difficult area in which to conclude international agreements since it is closely related to national security interests.

The art of cryptography has a long history. It dates back to the ancient Egyptians and has mostly been a tool of the State.[3] Cryptography is still used today to safeguard national security and foreign relations, hence the rigorous controls that always have surrounded the export and use of cryptography. The invention of the computer in the 1950s and the transformation of society from an industrial society to an information society have made society increasingly dependent on these networks of computers.

---

[1] *The Hutchinson Encyclopedia*, 8th Ed., (London: George Philip & Sons, 1988) "cryptography" at 332.
[2] See A. Michael Froomkin, " It Came From Planet Clipper: The Battle over Cryptographic Key "Escrow"(1 November 1996), online: University of Miami http://www.law.miami.edu/~froomkin/articles/planet_clipper.htm (date accessed: 14 October 1997).

These networks have in fact become the spinal cord of many industrialized countries and the communication backbone is today considered to be of vital national security importance.[4] The ease with which communications can be intercepted has further increased the necessity of protecting communication in all forms: e-mail, fax, and mobile- or Internet telephony. Today anybody with a scanner can eavesdrop on a private communication between two persons using cordless or cellular telephones.[5] The main question for governments is how to ensure privacy and at the same time enable lawful electronic surveillance.

On one side we have a legitimate national security and law enforcement interests and on the other side we have just as legitimate interests represented by businesses and people who feel that their security and privacy are too easily threatened in a modern information society. Because of the new applications for intercepting telecommunications, which have been developed, and moreover, the increased use of these new applications by many countries to conduct foreign industrial espionage, new cryptographic products have been developed to meet this threat to communication. A primary interest for national security agencies is to conduct counterintelligence to reveal and prevent foreign espionage. This task would be considerably easier if businesses were able to freely encrypt their confidential communications worldwide and thereby to protect their sensitive information.

Cryptography can, as all technological inventions, be used for both legitimate and illegitimate interests. An argument put forward by several governmental security

---

[3] About 4,000 years ago the Egyptians started to use hieroglyphics, which is a coded written language, See D. Kahn, *The Codebreakers: The Story of Secret Writing* (New York: Macmillan 1967) at 266 [hereinafter *Codebreakers*].

[4] The President's Commission on Critical Infrastructure Protection (PCCIP) was established by Executive Order 13010 and is advising the President of the United States on strategies for protecting and assuring critical infrastructures from physical and cyber threats. For more information on this subject refer to: "PCCIP" http://www.pccip.gov (date accessed: 25 October 1997).

[5] As opposed to eavesdropping, which a decade ago required access to the telephones or the telephone line eavesdropping currently only requires accessibility to a scanner. MI5 (A British Intelligence Agency) learned how to use ordinary telephones as microphones in the early 1950s. See P. Wright with P. Greengrass, *Spy Catcher,* (Victoria, Australia, Heinemann Publishers Australia, 1987) at 110 ff. Today intelligence agencies have an enormous capability to monitor and eavesdrop on all kinds of communication without physical access. This ability to access information is of course of vital interest to states. Global widespread use of strong cryptography could endanger this capability. For more information on this topic, see E. Ratcliff, "Spying on the Echelon Spy Network" (2000), Wired Magazine, online: Wired Magazine http://www.wired.com/archeive/8.04/mustread.html?pg=2 (date accessed 8 April 2000) It should be noted that modern digital mobile telephones usually are encrypted between the base station and the mobile telephone.

agencies is that unrestricted use of encryption would do more harm than good. However, this argument does not bear much merit when one looks at the whole picture. The overall drawbacks of being able to use only weak cryptography internationally widely surpass the implications for law enforcement and national security agencies. A compromise suggested by some states is key recovery, which means that the holder of the cryptographic key has to deposit the keys with a state depository. Several studies show, however, that key recovery will be extremely difficult to implement internationally, simply because it means giving up sovereignty, national security and control over vital national economic interests to some extent.

The efforts by the OECD to create a greater international consensus on these issues should be seen in the light of these developments. The OECD cryptography guidelines represent a step in the right direction even though the guidelines can be criticized as being too broad and vague. It remains to be seen to what extent the OECD guidelines will contribute to a global consensus concerning cryptography. The OECD Cryptography Policy Guidelines represents at least a small step on the way to international consensus.

The Paradox

Not very much has happened in terms of international harmonization since the OECD Cryptography Policy Guidelines were adopted. One might believe that since encryption has the potential of reducing crime substantially by preventive measures and increased privacy there should be a great incentive to agree on harmonization. So far other interests, such as national security interests, have been given more weight. I would argue that cryptography probably will reduce, rather than support crime. A widespread use of cryptography strengthens authentication procedures and makes it more difficult to gain unauthorized access.[6]

Despite the obvious benefits cryptography may bring, the use and export of strong cryptography are still surrounded by restrictive regulations. The main argument against the use and export of cryptography has been that cryptography presents a threat

[6] It might be argued that one has to differentiate between different types of cryptography, for example cryptography used for authentication purposes and cryptography used for confidentiality. One the other hand the basic algorithms are often the same. The difference lies rather in how the algorithms are used.

against law enforcement and national security. However, in what way the threat persists has never been explained fully and clearly. That pedophiles, drug traffickers and terrorists would benefit to an extent outweighing the positive features of cryptography in a wide sense is, at the mildest unrealistic. That it will have an impact on the possibility to wiretap is clear. To what extent that loss of capability will impede law enforcement agencies remains, however unclear. It seems that the real underlying reasons for restricting the use of cryptography relates to national security reasons. A major reason for the slow implementation of the OECD Guidelines in the USA seems to be the loss of intelligence capability that a widespread use of encryption might result in.[7] That is probably also a major reason why France has been restricting use and export of strong encryption.[8]

A Framework for the Research

The main subjects of this thesis are the international regulation of cryptography and the legal implications of cryptography, not computer and telecommunication security in general. The starting point is the OECD Cryptography Guidelines and how they have been, and should be, interpreted. An understanding of vulnerabilities, risks and other security measures is necessary to understand the legal and political issues and a brief introduction to some of the issues is therefore provided at the beginning of the thesis. Cryptography as such is not a stand-alone solution to a specific problem, but rather one method in a complicated and complex system. The role that cryptography will play to secure communication networks and enhance privacy remains to be evaluated and will to a large extent depend on the legal framework in which it operates.

This study does not cover all aspects of cryptography either. That would take the study too far away from the legal questions involved. The OECD Cryptography Guidelines therefore stands in the foreground as one of the few attempts that have been made to regulate cryptography. Also, the Wassenaar Arrangement and its forerunner

[7] The USA has built up an impressive worldwide intelligence service with a great capability to intercept communication. Information has at the same time become increasingly important for business and people. A widespread use of cryptography would severely impair this capacity. Of course, other intelligence services than that of the US would be impaired. However, the USA would be most affected since they have made the biggest investments in for example satellites.

[8] France reviewed their domestic regulation on the use of cryptography in 1999 and made them less restrictive.

COCOOM are discussed in the study in order to put the OECD Cryptography Policy Guidelines in a broader perspective. It should be noted that although the study tries to take a comprehensive approach, much of the focus will nevertheless be on the USA. This is mainly for three reasons: firstly the dominance of software products in the USA, secondly the economic and political power that the USA has, and thirdly the lively debate that still continues in the USA about encryption and the export of cryptography.

An argument heard in the public debate sometimes is that cryptography cannot be discussed thoroughly because many aspects are classified. It is my belief that even though some aspects may be classified it is still possible to have an open public debate. Most of the classified aspects relate to specific foreign relations or specific actions and movements. To argue that a debate is not feasible is not credible.

It depends on how it is used. Moreover, I feel that one should take an overall picture of the issues surrounding cryptography. The debate has until today been very much restricted to national security and law enforcement needs contra privacy and businesses needs. Cryptography itself cannot be considered bad or good.

PART I: The information society and the growing role of cryptography

This chapter describes briefly some of the issues that the increased use of information and communication technologies has brought us. These new technologies offer great possibilities – but also an increased vulnerability for society in general, to individuals and to business.

1.1. The Development of the Information Society

The transition from an industrial age to an information age was spurred by the globalization of business and led to an increased dependency on computers and communication technology (information technologies). The convergence of technologies has lead to more cost effective communications and increased connectivity. The major portion of GDP (Gross Domestic Product) in the industrialized countries no longer comes from goods but services. Affordable information technologies with new services have led to a step growth of the global telecommunication network and facilitate communication for individuals, business and the society as a whole. Global access is no longer rare. There is, however, a tension between openness and information technology security. To illustrate the above-mentioned some of the different interests are examined below. I will also discuss the risk and vulnerabilities this new society creates.

Development

Computers and computer networks have become an integrated part of the information society and enriched our lives in many ways.

> The benefits of the NII [National Information Infrastructure] for the nation are immense. An advanced information infrastructure will enable U.S. firms to compete and win in the global economy, generating good jobs for the American people and economic growth for the nation. As importantly, the NII can transform the lives of the American people-ameliorating the constraints of

> geography, disability, and economic status-giving all Americans a fair opportunity to go as far as their talents and ambitions will take them.[9]

The transition from an industrial society to an information society began with the growing use of computers in the 1950s. One of the first areas in which computers were used was in fact for cryptographic purposes by the military, hence the rigorous control of cryptography as munition.[10] The military used computers to break ciphers, also referred to as cryptoanalysis.

The development of the computer took off when new processes for manufacturing increasingly smaller and more powerful microchips and electronic circuits were developed. Computing power until recently doubled every 18 months. This trend called Moore's law has in the last few years been revised because of the unprecedented rapid development of computing power. Computing power is now estimated to double every 9 months.[11] Today, microchips are included in everything from household appliances to cars and fighter planes. The increased use of computers has been accompanied by a second important development, the change from an analog technology to a digital one. This change has led to an ongoing convergence of media and means of communication. Digital technology has created new forms of human interaction and new exciting emerging fields such as Internet telephony, webtv, videoconferencing, Electronic Data Interchange (EDI) and electronic cash.[12]

Technologies are converging and create new possibilities. A third important development in the transition from an industrial society to an information society was the connection of computers into networks and of those networks with other networks.

---

[9] R.H. Brown, chair National Information Infrastructure Task Force, September 15, 1993, National Information Infrastructure Agenda for Action. Available online at http://www.iitf.nist.gov/documents/speeches/brown.html (date acessed: 4 July 1997)

[10] The first computer in history, the Colossus was built to cryptoanalyze German ciphers as early as 1943. The England's Code and Cypher School developed this computer especially to target German codes. See G. Brassard, *Modern Cryptology- A tutorial, Lecture notes in Computer Science* (New York: Springer, 1988) at 2 [hereinafter *Modern Cryptology*]. See also J. D. Wallace, *Sex, laws and cyberspace: freedom and regulation on the frontiers of the online revolution* (New York: Henry Holt and Company, 1996) at 43 [hereinafter *Sex, Laws and Cyberspace*] (Munition is e.g. dual use good that can be used for both civil and military purposes.)

[11] According to Professor David Johnston. (Information given during a lecture. (19 November 1998)

[12] As always when new technology creates new markets and new possibilities friction emerges and the ones affected try to convince the Parliament that new legislation is necessary. There is an inherent resistance against new developments and furthermore, an interest to defend positions. An excellent example hereof is the development of the telegraph, which was meet with suspicion when it was

The United States research net, the ARPA net, lay the foundation for a global network of computers that is now known as the Internet.[13] The open network standard, the TCP/IP protocol, has spurred new applications, such as the World Wide Web (WWW) and Wireless Application Protocol (WAP). New information technologies, new computer and communication technologies have facilitated communication, which in turn has increased productivity and resulted in a boom economy.[14]

Vulnerabilities

The price we have had to pay to achieve this information society is an increased vulnerability for governments, business and individuals.

> In addition, it is essential that the federal government work with the communications industry to reduce the vulnerability of the nation's information infrastructure. The NII must be designed and managed in a way that minimizes the impact of accident or sabotage. The system must also continue to function in the event of attack or a catastrophic natural disaster.[15]

To facilitate the command and control of essential societal functions such as power grids, aircraft control, transportation systems, banking systems, medical, food and water supply many systems have been connected to communication networks and are controlled with the help of computers. Disruption of one part of the so called NII may cause cascading effects to other parts. The telephone system is for example dependent

---

developed. Today Internet telephony is emerging and established common carriers try to defend their positions.

[13] The ARPANET (Advanced Research Projects Agency) of the U.S. Department of Defense was originally developed for military purposes in the 1960s, but was later used for communication and research between universities. In 1991, despite much resentment from users, the Internet was opened up for commercial use. The World Wide Web protocol with its text-based search possibilities (hypertext) was specified in 1992. The first graphical net-search program, the Mosaic, was introduced in 1993. (O. Torvund, Elektronisk handel via Internet" in *Elektronisk handel –rättsliga aspekter, Nordisk årsbok i Rättsinformatik 1997*" (Stockholm: Nordstedts Juridik, 1997) at 2. In 1998 the Internet had more than 120 million users. (T. Carlén-Wendels, *Nätjuridik-Lag och Rätt på Internet*, 2d ed. (Stockholm: Norstedts Juridik, 1998) at 35 For more statistical information about the Internet see http://www.nw/zone, http: //www.ripe.net/statistics/hostcount.html and http://www. nua.ie/surveys (Since the number of users doubles every year, old statistics might not be that reliable.)

[14] According to an industrial analysis released by Forrester Research on 19 August 1998 (Media's Global Future) online advertising will rocket upward from US $2 billion 1998 to $15 billion in 2003. Spending on the Internet, Forrester predicts, will rise steeply from $105 million 1998 to $2.8 billion in 2003. If the prognosis holds true, per capita spending on the Internet will have surpassed several other important media such as magazine and radio in only five years. For more information on this topic see "Europe to Drive online Boom", http://www.wired.com/news"business/story/14511.html, (date accessed: 20 July 1998)

on power from the power grid. The power grid is on the other hand controlled by telephonic communications and if the power grid stays off-line for more than 10 days it could cause massive telephone failure making it in turn impossible to control the power grid.[16] The system has become so complex and dependent on communication that even a small failure or loss of telecommunications might result in incalculable consequences.

Not only civilian authorities have become dependent, but also to a greater and greater degree the military establishment; "...the threat to our information systems will grow in coming years as the enabling technologies to attack these systems proliferate and more and more countries and groups develop new strategies that incorporate such attacks".[17]

In the United States the Department of Defense (DoD) has moved towards a globally integrated Defense Information Infrastructure (the DII) to fully explore the advantages of information warfare.[18] Command and Control warfare[19] is today highly developed and requires reliable, accurate and globally available real-time information systems. The U.S Army's Chief of Staff has called operation Desert Storm the knowledge war because of the intelligence power the alliance had compared to Iraq.[20]

Governments are taking these threats to the information society seriously and computer and information security is currently on the top of the governmental agendas. It should also be kept in mind that an increasing number of public networks are connected to the Internet and therefore can be accessed by anyone else connected to the Internet- unless protective measures are in place. Any business, regardless of size, is dependent on computers for a wide range of duties such as keeping control of payrolls, employees, retirement plans, payables and receivables. Security of computer networks

---

[15] *Supra* note 9

[16] F. Cohen, *Protection and security on the information superhighway* (New York: John Wiley & Sons, 1995) at 6 [hereinafter Cohen]

[17] J. Deutch, "Goals", National Security Agency, http://www.nsa.gov:8080/programs/ncs21/goal1.html (date accessed: 22 July 1998) Dr. John Deutch, former Director of Central Intelligence

[18] *Supra* note 16 at 27

[19] The destruction of communications in Iraq had a massive impact on the Iraq economy and attacks against command and control systems to weaken the ability to fight were part of the doctrine. Because of the integrated military and civilian use of telecommunications the civil population is as much affected as the armed forces currently. Destruction of infrastructure such as telecommunication facilities is a legitimate military target. The effect of this destruction is great on the civilian population. The inventory, supplies and logistics of the defense forces in the U.S. have been automated with information systems to provide coordinated logistics and is today very dependent on information systems. An operation like the Desert Storm required an enormous logistical capacity and transport system.

and information systems has also become vital for business. It does not, however, matter how good the managerial, physical and operational security is if security policies are not being followed. There are numerous examples of security breaches that have led to illegal intrusion into networks that were believed to be secure.

One of the factors still holding electronic commerce back is the lack of security of transactions over the internet.[21] AT&T claim the company lost $2 billion in 1992 because of computer fraud and the FBI estimates computer crime accounts for $5 billion annually.[22] The ease with which confidential information and communication can be gathered and intercepted has led to a loss of security in the information society. New technology has, moreover, resulted in legislation covering no longer what people conceive to be criminal behavior. An American court for example, did not consider the eavesdropping of a politician's conversation over a cellular phone by a reporter as illegal because, according to the court, there was no expectation of privacy. The conversation could be intercepted by anyone with a scanner, concluded the court. The telephone call was therefore comparable with broadcasting. Conversation over telephones by wire is well protected in most countries, but the law has not always protected it. It always takes time for the legislator to catch up with new technology and until he does, a legal vacuum exists. Since criminal law shall be interpreted restrictively it is in most cases up to the legislator to close loopholes opened up by new technology.[23]

---

[20] Alan D. Campen, ed. *The First Information War* (New Jersey: AFCEA International Press, 1992) at IX

[21] In a white paper; "Electronic Commerce: Analysis of a New Business Paradigm", (1997) Internet Business, 7 August 1997 at 38 JCP Computer Services has identified the biggest stumbling block to electronic commerce—security on the Internet. According to the study, the chief concern of business and customers on the net is security. The study concluded that knowledge of the technologies involved is limited. Once the security problem is solved, massive potential cost savings and new ways of targeting advertising and marketing are waiting. Electronic commerce will make trading feasible for small and much easier for larger companies. The Internet is not and will never be a safe place to conduct business, however. It is an open unsecure network and it is therefore accessible for hackers and viruses. The same criminal activities that surround us in our every day life, which we have to be careful about, will also be found on the Internet. Some of the risks are; fraud, eavesdropping, and interception of confidential messages. The use of 'export crippled' cryptography and poor security implementation opens up vulnerabilities even more for criminal intentions.

[22] *Supra* note 16 at 2

Cryptography's role

A new application of an old technology- cryptography- can serve to bridge this gap between a reasonable expectation of privacy and the lack of security from the user's perspective. [24] However, use of strong cryptography for confidentiality purposes may pose difficulties for governments as it renders it impossible in most cases for law enforcement agencies to decrypt information acquired through wiretapping. Encrypted information also makes it difficult for national security agencies to conduct cryptoanalysis and intercept information on telecommunication lines.[25] An important question is whether there is a primary right to conduct wiretaps and eavesdrop or if the primary right is to be "left alone". Which has priority over the other? The debate about government intrusion has raged in the United States since the failed attempt by the Clinton administration to introduce the Clipper chip. The Clipper chip debate made governments and individuals in the rest of the world aware of cryptography and made cryptography an issue on the political agenda. Some countries did not welcome Cryptography becoming visible. Cryptography is still considered as subject *non grata* in many countries.[26]The next part of this thesis describes the technology behind cryptography, its use and possible misuse.

---

[23] Internet telephony represents another leap forward. Since Internet Telephony is a packet switching technology over open networks it will be harder to regulate than traditional telephony, which traditionally has been heavily regulated.

[24] It can be argued that the absence of legislation regarding privacy and security has led to the present situation. The use of strong encryption for confidentiality purposes and the eventual disadvantages that strong encryption might have for national security and law enforcement agencies could have been avoided if the legislator had reacted earlier and more powerfully. In particular in the USA and Canada where privacy legislation for the private sector is poor. In Europe and in particular within the EU a much firmer stand has been taken regarding privacy.

[25] The reason is that encrypted messages will no longer stand out from the usual flow of data. (When only a small portion of all communication is encrypted, encrypted data is standing out in the data flow, i.e. encrypted messages are identifiable and are more resources can be spent on encrypted messages. If all communication, regardless of sensitivity, is encrypted it will be much more difficult to identify and decipher all communication)

[26] In France and Belarus the use of encryption is subject to governmental licensing. (Franc Loi no 90-1170, du 29 decembre 1990 (Art. 17 amending Article 28. France has recently amended the regulations regarding cryptography. Regarding Russia, see Edict No. 334 of the President of the Russian Federation on measures to Observe the Law in Development, Production , Sale and Use of Encrypting Information (April 1995) For more information on this topic see S.A Baker & P.R. Hurst, *The Limits of Trust Cryptography, Governments and Electronic Commerce*, (Cambridge, MA: Kluwer, 1998) at 407 ff and 525 ff)

1.2 Information- and Computer Security

In order to understand the role of cryptography it is necessary to have a basic understanding about information and computer security in general. Some problems with new cryptographic technologies and difficulties in legislating on them will be outlined below. Information and computer security can only be the result of combined efforts – technical and organizational as well as legislative. Network security can roughly be divided into two parts: protection against active attacks (falsification of data and transactions) and protection against passive attacks (eavesdropping). Cryptography can be used for both the above mentioned purposes. It can e.g. be used to protect computer networks from unauthorized intruders and hackers in a firewall. A firewall is a scheme of measures taken to prevent unauthorized access to a computer network through, for example an authentication scheme such as a one-way function.[27] Usually a firewall is set up as a "first line of defense." Security does, however, not exist in a vacuum , a well-defined set of norms and laws is required to make it effective and enforceable. Without an existing set of actively enforced laws it would be very hard to achieve a high degree of security. Several public services are, for example, used with an assumption that they are safe. The postal service is e.g. presumed not to open any letters. It is, furthermore, assumed by the general public in a democratic society that telephone calls are confidential and that nobody is listening to them, an assumption that is not always valid.[28] It is therefore important that the surrounding set of laws and norms keep up with new technology and new developments. The legislator faces difficulties when new technology is introduced, since new technological applications cannot always be subordinated to existing laws. Should e.g. an Internet telephone call made through the Internet between two computers be regulated using telecommunication legislation or should it be judged as any other Internet traffic? A

[27] Something that is easily forgotten is that the information, rather than the system should be protected. Usually the information is worth considerable more than the computer network. This has to be kept in mind when security measures are taken. A perhaps more useful approach is therefore to determine security levels for the information in the network rather than only focusing on unauthorized access. Highly sensitive and confidential information might have to be encrypted and access restricted, while publicly available information does not need very much protection on the computer network. Another issue is of course measures to keep unauthorized persons away from access to the root library and from taking control over the network.

[28] Telephone calls made using a cordless portable phone can easily be intercepted and eavesdropped on with a simple scanner.

host of new and intricate regulatory problems meet the legislator when new techniques are introduced. On one hand there is an inherent risk that the market demands that providers and manufacturers encrypt all traffic if adequate legal protection is not offered by the legislator. On the other hand there is also a danger in reacting too fast and establishing a standard that is not technology neutral and thus will hinder instead of support. The right approach is therefore, in my view, for parliaments to legislate step by step while trying to keep up with new technological developments and market developments. Regulating cryptography and the use of cryptography is very difficult since international agreements have to be concluded. Cryptography is furthermore an area in which user confidence is essential. Governments therefore have to make sure that suggested legislation is accepted by the majority of personal users and businesses.

Developments

One ongoing development is the move from paper-based documents to digitally stored documents, which creates problems in terms of the legal standing of documents. Documents may be something as complex as the Electronic Data Interchange (EDI) or an attachment to an e-mail in the form of a contract. The main difference between an electronic document and a paper document is that a digitally stored document can easily be reproduced and altered without leaving any traces. A paper document will always bear witness if it has been tampered with, although such signs might not be visible to the eye. A digital signature can thus be of great help for the society by refining the legal qualities of a paper document. Use of a digital signatures, which is described further in the next part, will therefore probably enhance information security and reduce opportunities for fraud.

PART II AN INTRODUCTION TO CRYPTOGRAPHIC HISTORY, TECHNIQUES AND METHODS

2.1 Cryptography-New Applications of an Old Technology

2.1.1 The history of cryptography[29]

Cryptography has historically been considered to be more of an art than a science. Modern cryptography has, however, not much in common with art anymore. The work with breaking cryptographic system and the development of new systems was captured by Voltaire in the 1700s."Ceux qui se vantent de lire les lettres chiffrées sont des plus grands charletans que ceux qui, se vanteraiant d'entendre une langue qu'ils n'ont point apprise".[30]

It is said that Julius Caesar did not trust his messengers so he first encoded the messages.[31] The cryptographic method he used was very simple. Replace the letter in the message with the third letter following in the alphabet. This simple scheme is called a crypto or cipher system and was one of the first known cryptographic systems.[32] The next major step in the cryptographic history was the development of the Polyalphabetic encryption that came to be named, erroneously, after Blaise de Vigenère.[33] A very

---

[29] For an excellent review of the history of Cryptography see , *The Codebreakers supra* note 3, R. Ceillier, *La cryptographie,* Que sais-je?, vol. 116 (Paris: Presses Universitaires de France, 1945), H.O. Yardley, *The American Black Chamber* (Indianapolis: Bobbs Merrill, 1931, reprinted by Ballantine Books, New York), P.Wright, *Spycatcher* (New York:Viking Penguin, 1987), C.A Devours, "Unicity Points In Cryptanalysis" (1977) vol 1 Cryptologia, J. Garlinski, *Intercept: The Enigma War* (London: J.M. Dent and Sons, 1979), D. Kahn, *Kahn on Codes* (New York: Macmillan, 1983) For a more recent review of cryptography and cryptographic history see W. Diffie & S. Landau, *Privacy on the line: the politics of wiretapping and encryption* (Massachusetts, Cambridge: The MIT Press, 1998) [hereinafter *Privacy on the Line*]

[30] Voltaire (F.-M Arouet), *Dictionnaire Philosophique* (Paris:1769)

[31] Seth Godin, *Presenting Digital Cash*, 1 ed. (Indianpolis: Sams.net, 1995) at 47 [hereinafter *Digital Cash*]

[32] This is a technique called simple or monoliteral substitution. In a 26-character alphabet there are 2^{90} possibilities. Thus 90-bit key sounds quite safe, but since many characteristics, such as letter frequency and patterns, always can be recognized by a cryptoanalyst such a keyspace is not as reliable as one might think. Cryptoanalysts can recognize all these special characteristics and letter patterns that all languages have and by the help of these clues analyze an encrypted message. The letter E accounts e.g. for 13 % of all letters in an English text and the letter Z for only 1 %. An exceptional word like "bookkeeper", which in fact is the only English word with three double letters in a row, might be read out directly from the ciphertext by a skilled cryptoanalyst. Words that can be read from both directions-palindromes-are especially easy to figure out. (For more information on this subject see *Privacy on the Line supra* note 29)

[33] The actual inventors were three Renaissance scholars; Alberti, Belaso and Trithemius. See *The Codebreakers , supra* note 3

simple Vigenère cipher is the direct standard alphabet.[34] One alphabet is used to encrypt the first letter, another to encrypt the second letter and so on. Each one of the alphabets is labeled by a letter and the key to the cipher is the phase formed by the sequence of alphabets used. The security of the alphabet is dependent on the length of the message as well as the length of the key. One way of increasing the difficulty of breaking the cipher is by encrypting it more than once- a technique used today in the triple DES (Data Encryption Standard).

As time went on it was discovered that multiple encryptions could be done more easily if a rotor machine was used. By simply turning the handle the message could be encrypted once more. Examples of rotor machines are the Hagelin and the Enigma, which were used by the Germans during the Second World War. The British broke the key of the latter with the aid of Swedish mathematicians during the Second World War. Once the first computers had been built shift register encryption schemes were developed. The DES is a variant of a traditional shift-register encryption system. Today, increasingly complex encryption systems are used such as block ciphers, stream ciphers, random sequence ciphers and public key ciphers. The different systems have different advantages and disadvantages as well as usages. Some ciphers such as public key algorithms for example are usually slower than block ciphers making them less suitable for continuous encryption. An advantage with the public key system is that it provides means of sending information through a "secure tunnel", a channel that can be established without previous contact. Hence a session key can be sent with a public key system and then the session key can be used to encrypt the longer message faster than the public key system itself is capable of.

2.1.2 Landmarks in modern cryptography

One important landmark in modern cryptography is the work of Feistel at International Business Machines (IBM) in the beginning of the 1970s.[35] His work for IBM led to IBM's algorithm being accepted as the U.S. Federal Information Processing Standard (FIPS). Another leap forward in the cryptographic history is the Data Encryption

[34] *Supra note 29* at 22 ff

[35] For a description of the DES algorithm see U.S.A, Gaithersburg *Conference on Computer Security and the Data Encryption Standard, Computer Security and Encryption Standard*, (National Bureau of Standards Special Publication Paper 500-27) (Washington :U.S. Government Printing Office, 1978)

Standard (DES) adopted in 1977. Another landmark is the concept of public-key cryptography that Diffie and Hellman published in 1976 in a revolutionary paper, *New Directions in Cryptography.* The paper solved the problem of transferring the keys in symmetric cryptography on open networks by inventing asymmetric cryptography, in which two different keys were used, one private and one public. Rivest, Shamir and Adleman developed the idea of public key encryption further to the first practical public key and encryption scheme.[36] The RSA algorithm, named after them, forms the base for the first International Standard for digital signatures, the ISO/IEC 9796 standard. The present U.S digital signature standard is based on the ElGamal public-key scheme originally discovered by ElGamal in 1985.[37]

Since civil cryptography took off about 20 years ago many new algorithms have been developed. There is, however, a constant struggle between cryptographic developers and cryptographic breakers. Computing power plays an important role in this ability to break a cryptographic algorithm. As increasingly powerful computers are developed more and more complex calculations can be done in the same time. The faster computers get, the more easily cryptographic systems can be broken. Computing power is especially important when a brute force attack is conducted. In a brute force attack all possible keys are tried in a process of trial and error. Also important to break cryptographic systems are resources in the form of skilled cryptoanalysts.

To summarize, the more computing power, time and cryptoanalysts at one's disposal the less time it will take to break a crypto system. One of the most common cryptographic algorithms, the DES, has become vulnerable as a result of increasing computing power. Most cryptographic algorithms with a minimum key length today are considered to be so hard to break that it is not feasible with the present available computing power to break them.[38] Breaking them would simply take an eternity. Some cryptographic systems are moreover unbreakable by definition.[39]

---

[36] A. Menezes, P. Oorchot, S. Vanstone, *Handbook of Applied Cryptography*, (Florida: CRC Press, 1996) [hereinafter *Menezes*] at 2

[37] The El Gamal algorithm is based on a discrete logarithm problem. *ibid* at 2

[38] I do not consider DNA computing or other methods with great potential, but not yet fully developed. DNA computing may in the future be a practical way to solve complex algorithms, but it is still just a great promise and no one knows if will be useable.

[39] One-time pads are per definition unbreakable, even given infinite resources, because the keys are randomly chosen and only used once.

Encryption systems have until the most recent years been of military interest only. When we are moving into a more global and networked world, as described in Part I, the importance of privacy and confidentiality becomes increasingly important. The level of security of an encryption scheme has to be viewed in relation to the value of the information that can be gained if the information is lost or stolen.[40] Basically, hardware encryption, i.e. a encryption program built into a chip is usually faster than software encryption run by an application program. Private-key encryption (i.e. symmetric cryptography e.g. DES) is, moreover, faster than public-key encryption (i.e. asymmetric cryptography e.g. the RSA used in the PGP (Pretty Good Privacy)[41] program. For encryption in real-time, hardware encryption is most frequently used. An example of a hardware encryption application is the Clipper chip.

2.1.3 A basic introduction to cryptographic techniques and methods

It is important to stress that cryptography is not the only way to secure information. Nor either is cryptography the only part in a secure information system. It is, however, an important part, used increasingly for many purposes. Therefore, it is necessary to develop a global standard to support information exchange. Cryptography today provides an important tool and more applications using cryptography will probably emerge as cryptography helps the user to regain control over his communication and information. Historically cryptography has been considered to be munition and therefore subject to national and international regulation.[42] This is slowly changing.

Cryptography can of course, as all technology, be both used and misused. What constitutes misuse is open to interpretation and depends on the perspective. From a user perspective cryptography can be divided into four subgroups, depending on for which purpose it is used; encryption, data integrity, authentication and non-repudiation.[43] Below is a flowchart of different kinds of cryptographic techniques and methods and

---

[40] *Supra* note 36

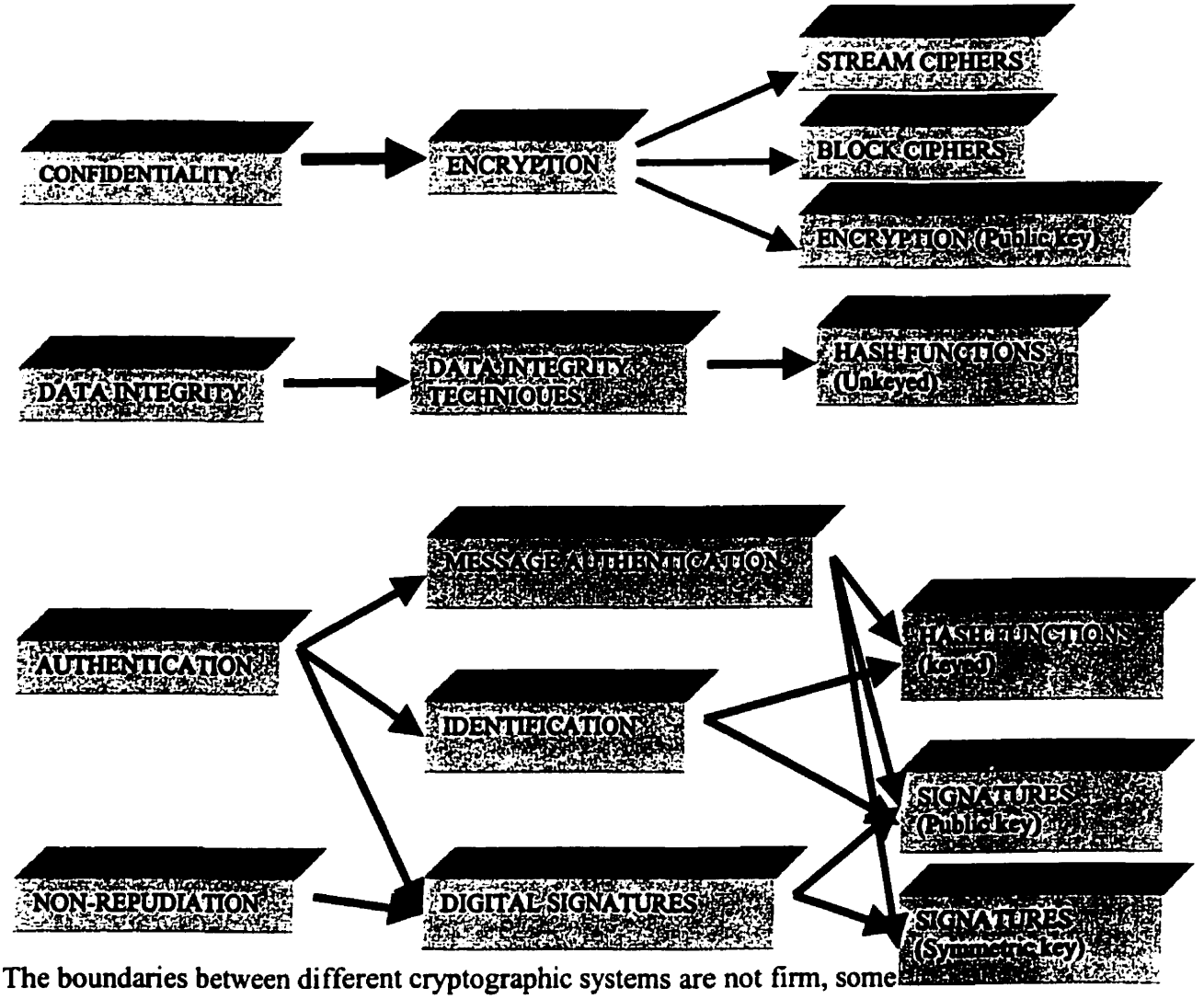
[41] Arnold G. Reinhold *Internet Privacy and Security* in John R. Levine & Carol Baroudi, *Internet Secrets*, 1 ed. (New York: IDG Books Worldwide, 1995) at 130

[42] The CoCoom agreement which regulated export of technology to certain countries has been replaced with the Wassenaar Arrangement, which in December 1998 was amended. The Wassenaar Arrangement is now implemented in the European Union through EFT 1999 L73 adopted by the Council of Ministers March 9, 1999 (See "Wassenaar-aftalen indført i Danmark", (1999) Nr 59 (September) *Lov & Data, at 18*

[43] See further Chapter 2.2.5.

their possible uses and purposes. Only the most important ones will be described in the text. The interested reader should consult Bruce Schneier, *Applied Protocols, Algorithms, and Source Code in C* (New York: John Wiley & Sons, 1996) or for a more technical book Alfred Menezes, Paul von Oorchot, Scott Vanstone, *Handbook of Applied Cryptography* (Florida: CRC Press, 1996).

2.1.4 Cryptography systems and methods from the user perspective[44]



The boundaries between different cryptographic systems are not firm, some cryptographic methods can be used for more than one purpose. It is, nevertheless important to understand one fundamental distinction: the distinction between cryptographic systems used for confidentiality purposes and cryptographic systems used for authentication, data integrity or non-repudiation. It is only cryptographic systems

[44] See *Menezes, supra* note 36 at 4

used for confidentiality purposes that might pose a threat to national intelligence and law enforcement agencies. Cryptographic methods used for the latter purposes will probably reduce the possibility to commit crime since they can be used to seal documents and trace documents to a certain user. In due time cryptographic methods will probably reduce forgery and fraud. The mathematical foundation of the different cryptographic systems, methods and techniques are very technical and outside the scope of this very brief introduction to cryptography. An interested reader should consult the books mentioned earlier.

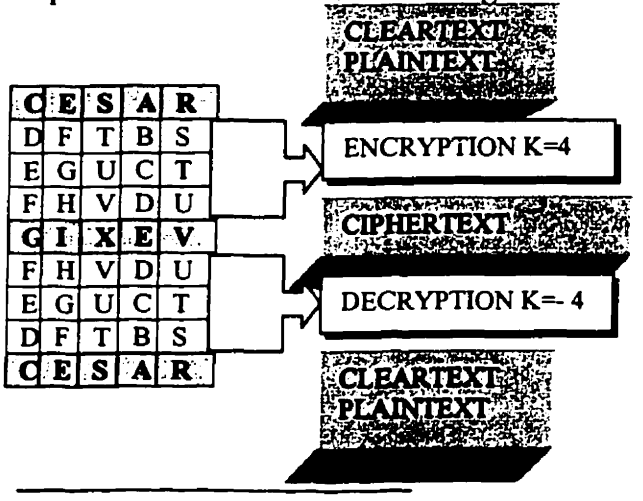
2.2 Cryptographic techniques and methods

2.2.1 Basic Cryptographic concepts[45]

To explain how cryptography works the cryptographic system allegedly used by the Roman emperor Julius Caesar may be taken as an example.

Caesar used a simple symmetric system: He replaced a letter in the message with the third letter following in the alphabet. The encryption key was thus K=3. Crypto systems in which the same key is used to encrypt and decrypt are called symmetric crypto systems, or sometimes, conventional crypto systems.

Let's say Caesar wanted to encrypt his name and use the key +4. Assume he wrote his name Cesar and therefore replaced the letter C with the fourth letter following in the alphabet C-D-E-F-G. He then changed the E etc.

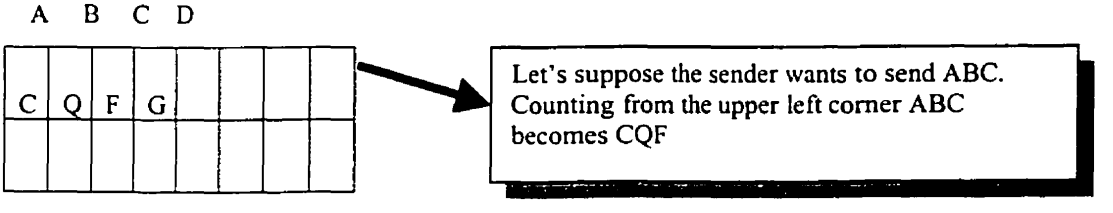


[45] There is a difference between coding and cryptography. Coding is a way of replacing words or phrases with codes that has been agreed upon beforehand. By coding a message the message gets shorter. Coding can therefore also be used to compress messages. Encryption on the other hand encrypts the whole message or a part of it, by using a mathematical algorithm. Coding is less secure than encryption because the coded text resembles the plaintext and can therefore be guessed. The structure and patterns in the message remains moreover if the message only is coded.

The Caesar cipher is a symmetric cryptographic system since both the encrypting key (encipher) and the decrypting key (decipher) are the same.[46] The Data Encryption Standard (DES) is an example of a widely used symmetric cryptographic system. The U.S government is currently in the process of replacing the DES with a more secure system.[47] We will now move on to look at some basic cryptosystems.

One Time Pads[48]

A very secure system, at least in theory, is the one time pad cryptographic system. In this cryptographic system doublets of randomly chosen keys are created. Because the pads are only used once, and the keys are randomly chosen, it is computationally infeasible to break the cryptographic system. There is simply not enough information to break the keys. The drawback of the system is of course key distribution, and moreover, that the information has to be adapted to the keypads. The keypads can have many variations. One variation is two identical sheets of paper with boxes. In the boxes letters from the alphabet and numbers are inserted. The order of the letters and numbers that becomes the keys has to be truly randomly chosen using, for example, a die. If, for example, the die shows C, Q, F and G when thrown. We fill the boxes with the letters starting from the upper left corner. After that an encryption scheme or key has been agreed upon we can start using the system.

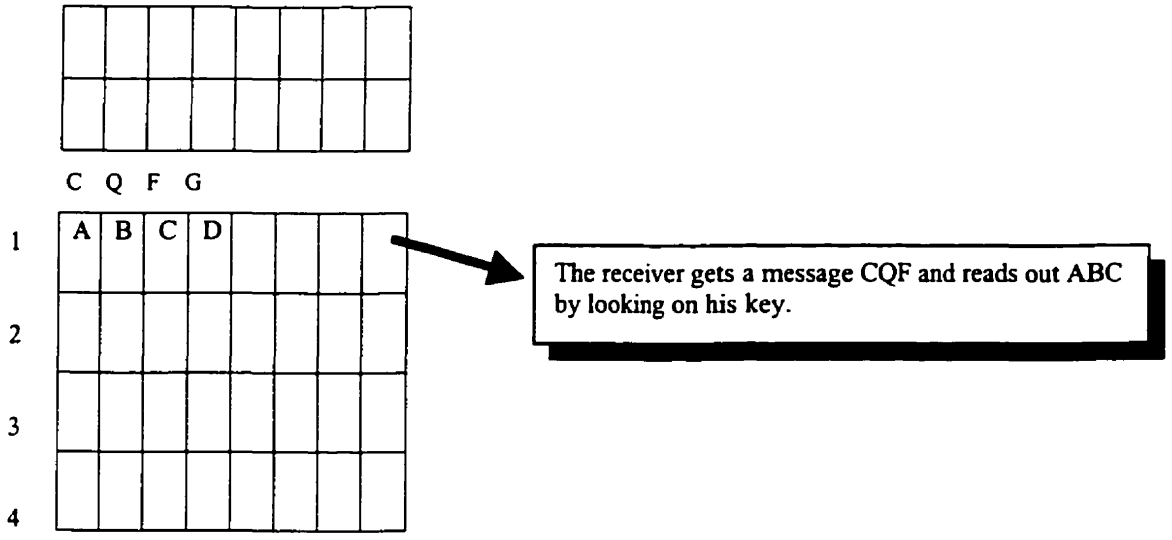


3

4 [46] The ISO 7498-2 standard uses the term encipher and decipher. See B. Schneier, *Applied Cryptography: Protocols, Algorithms, and Source Code in C, 2nd Ed.* (New York: John Wiley & Sons, 1996) at 1. [hereinafter *Applied Cryptography*]

[47] See "Feds relax crypto rules" Wired Magazine, September, 1998 available online at http://www.wired.com/news/news/politics/story/15037.html (date accessed: 18 September 1998)

[48] One-time pads were the primary cryptographic system for Soviet diplomatic communication from the 1920s to the 1950s. Because of carelessness with the one-time pads the pads became used more than once. That enabled the U.S.A. to break the messages in a project called Verona. On a large scale it becomes extremely difficult with key management in relation to one time pads. The Soviet solved this by having a very centralized communications and key management. See *Privacy on the Line* at 19ff. See also "Project Verona"(1998) online: http://www.nsa.gov:8080/ (date accessed: 1 November 1998)



Stenography -A non-encryption possibility to hide material

Even though cryptography has received most attention, it is after all not the only method to hide information. Strong encryption makes it if not impossible at least very difficult for law enforcement agencies to identify files with, for example, illegal material such as child pornography, irrespective of whether the material is stored on a hard drive or transmitted in some way. It is hard to positively identify files that are being transmitted because they are sent as packages from one router to another router. It is, however, possible. If e.g. the photos are encrypted before they are being sent it is virtually impossible to see what is being sent. Thus encryption opens up a possibility for illegitimate use. New technology always opens up new possibilities for both legitimate and illegitimate purposes. When photography was developed, so called French pictures quickly became popular and photography was declared to be the evil incarnated.[49] The World Wide Web has quickly been adopted by the pornographic industry and some people therefore see the World Wide Web itself as the incarnation of the evil. This is of course not the case.

Stenography and confidentiality

Confidentiality can be achieved in many ways. One way to achieve confidentiality is to use stenography. Information can be disguised, for example by hiding data in a picture

[49] French pictures were pictures of pin-ups.

or in another file. Information can, furthermore, be sent using a very low frequency that the human ear cannot distinguish. The information is protected by hiding it and making it difficult to detect, as compared to encryption where the protection consists of the message having been scrambled in an intelligent way. The difficulty of recreating the plaintext in a cryptographic system lies in the complexity of the algorithm and the length of the key.

Stenography, a way to hide files within other files can be used to achieve confidentiality as an alternative to cryptography. The high-order bit of the eight-bit bytes used to encode images are not used by many image formats and these unused bits can therefore be used to store e.g. a picture within another picture.[50] It is quite common among hackers to use for example university networks to store information.[51] The information stored can be hidden using stenography or encrypted so only persons with the key can access the information.

Also web pages can be used to hide information. The background picture can be used to hold information invisible to all but the initiated. Sound files can also be used to hold information simply by recording information at a very low pitch with a very low intensity sound.[52] For someone who does not know, the sound file only appears to be a melody. If it is analyzed, however, it reveals additional information.

2.2.1 Capabilities of Cryptographic Systems

Cryptography can improve several qualities that are attributed to a paper document. I will below describe the most important.

Authentication- verification

We are using authentication in our daily lives although we are not always aware of it. We authenticate ourselves with our voice, our signature or a PIN code. In a digital economy, however, the requirement of authentication is growing much more important

[50] N. Barett, *Digital Crime: Policing the Cybernation* (London: Kogan, 1997) at 74 [hereinafter *Digital Crime*]

[51] Kevin Mitnick, a well-known hacker used university networks to store source code to cellular telephone systems. Hard disk memory is expensive and there is always the risk of disclosure. By storing the illegal material on a network the hacker can get access to much memory space and does not risk being caught with the illegal material.

since we are more anonymous. The authentication process needs moreover to be faster and more secure. It should be noted that an authentication scheme does not necessarily have to reveal an identity, it merely needs to authorize access. In a financial transaction ,for example, our personal identity does not always have to be revealed, only our financial status, i.e. whether we have adequate funds to make the transaction.

A cryptographic authentication can also be used e.g. to deal with money laundering by including a source of the information, thereby making the relevant personal information traceable. If someone has gotten unauthorized access to your personal data and is using it, then the wrongdoer can be tracked down. The problem lies in ensuring that the cryptographic signature is not removed. There is of course always a possibility that someone retypes the information to get rid of the signature.[53]

A message is said to be authentic when:

A) its content has not been altered and

B) its source is verifiable[54]

The verification may also include the message's timeliness i.e. that it has not been artificially delayed and/or replayed. Nor has the sequence relative to other messages flowing between two parties been changed.
Authentication can be achieved by using conventional encryption. However, conventional encryption only protects the parties from a third party. It does not protect the parties from each other. Consider the legal implications of the following scenarios.

Alice transfers a contract to Bob electronically with detailed descriptions of a superior invention Alice has not yet patented.

---

[52] For a more extensive explanation of different methods used, see P. Wayner, *Disappearing Cryptography* (London: AP Professional, 1996)
[53] See further Kenneth W. Dam , *Cryptography's Role in Securing the Information Society*, (National Research Council, Computer and Telecommunication Board) (Washington DC: National Academy of Sciences, National Academy Press, 1996) at 370 [hereinafter *Crisis*] at 369
[54] William Stallings, *Make it real,* in Networks 2000 Internet, Information Superhighway, Multimedia Networks and Beyond, 1st ed. (New York: Miller Freeman,. 1994) at 305

1. If Alice and Bob are using conventional encryption and sharing the same key then Bob can forge an authenticated message and claim that it came from Alice. Bob could, for example send a contract to someone and claim that it came from Alice. In this case it would be difficult for Alice to prove that she did not send a contract.

2. On the other hand can Alice repudiate a contract if she decides that she does not wish to be bound by the contract and allege that Bob forged the contract even though it is authentic as to the form.

Conventional symmetric encryption can, as the example above illustrates, only be used if both parties trust each other. Otherwise it is of limited value in the absence of other precautions being taken. This possibility to repudiate a message or a contract is not possible with public key cryptography.

Measures that can be taken to authenticate a document

One way to avoid repudiation of documents is to have a procedure by which it is possible to verify the sender, the date and the time. This can be done by using a "time stamp" sent with the message. The parties can by such a "stamp" authenticate the content in the time the message is signed. By this procedure the message is sealed as at a certain time. Compare it with the function of a paper contract. The procedure must, however, be verifiable by any party relying on the authentication. Usually authentication is provided by a trusted third party, who signs the message with a digital signature.

A digital signature can both authenticate the message and verify it as to time and place. It is, however, not a copy of a written signature. Such a signature does not have any legal value. It is merely an electronic stamp that is fixed once it has been attached. Once the digital signature has been added to a document it cannot be deleted or changed without such tampering being detected. What we should try to achieve is not merely a secure document that has all the advantages of a paper-based message, but a digital document that is superior to it.

Message authentication code

This process is similar to encryption but with the difference that the authentication algorithm need not be reversible.[55] The authentication technique is based on a common key that both parties posses. When Alice sends a message to Bob a message authentication code is calculated as a function of the message and the key. When the message and the key reaches Bob the same calculation (based on the same algorithm) is executed and the two message-authentication codes are compared to each other. If the two message-authentication codes match each other then the message has not been altered. A number of algorithms can be used to generate such a code. The National Bureau of Standards has recommended the use of the DES algorithm.[56] The DES algorithm is used to generate an encrypted version of the message and the last bytes of ciphertext are used to generate a 16- or 32 bite code.[57]

One-way hash[58] *function*

A variant of the message-authentication code is the one-way hash function. However, no secret key is involved. It is simply a mathematical function that produces a known output for a given input by using an algorithm. (One-way because it is easy to create from the hash input but impossible to reconstruct the input from the hash.) One usage of a one-way hash function is to verify documents in, for example, a lawyer's office.[59] Legal documents could have a hash stamp that identified date, time and signing parties. An advantage with this method is that it is easier to compute than the message-authentication code. The disadvantage is that some measures have to be taken to protect the hash function and the message in order to provide authentication.

---

[55] *Ibid at* 306

[56] *Ibid* at 307

[57] Rumors have persisted that NSA influenced IBM's design of the DES. Suspicious has been directed on the so-called s-boxes in the algorithm that have been classified by IBM. See further P. Kinnucan, " Data Encryption Gurus: Tuchman and Meyer", vol. II, no. 4, Cryptologia, at 371. The authors of the DES have denied that NSA has been given information about a backdoor to the algorithm. G. Hyatt, "Stump the Cyberpunks" *Supra* note 54 at 24 [hereinafter *Hyatt*]

[58] A hash can be described as samples from a message collected intelligently by an algorithm.

[59] B. Schneider, *One-Way Hash Functions*, Dr. Jobb's Journal, Sept 1991 (New York: Miller Freeman , 1991) at 151

By using an algorithm to generate a fixed-size tag (*message digest*) to the message and then comparing the message digests included in the message with the generated message digest the authenticity of the message can be verified.

The message digest can be encrypted with either conventional cryptography or public-key encryption. However, a technique that involves no encryption may be preferable in many cases. A technique that does not involve encryption is to share a secret value.

Instead of sharing a secret key, calculated by an algorithm, the parties can share a secret value (SAB)[60]. When Alice sends a message (M) to Bob the hash function is concatenated by the secret value and the message (MH). When the message with the concatenated value is sent to Bob he is able to verify the authenticity of the message since he is able to recompute the message MH by using the shared secret value. As long as the secret value is not compromised the message can not be altered without knowledge of the parties. It is, however, of utmost importance that the secret value remains secret and that the value is used only one-way. If an third party is able to eavesdrop and intercept the transmission he can obtain the hash code and the message.

Digital signatures and public key systems

One method of creating a digital signature is to use public-key encryption. The Public key system was introduced in 1976 at Stanford University and is based on asymmetric keys, which means that the keys used to encipher and decipher are not the same.[61] The algorithm is, however, designed in such a way that it is virtually impossible to derive the other key even though a mathematical connection exists. The two keys can be used in either order.[62] If one just wants to create a digital signature one can use the private key to encrypt and the public key to decrypt the message. The public key is distributed and freely available. Both keys, however, use the same algorithm to encrypt and decrypt.

---

[60] *Supra* note 54 at 308

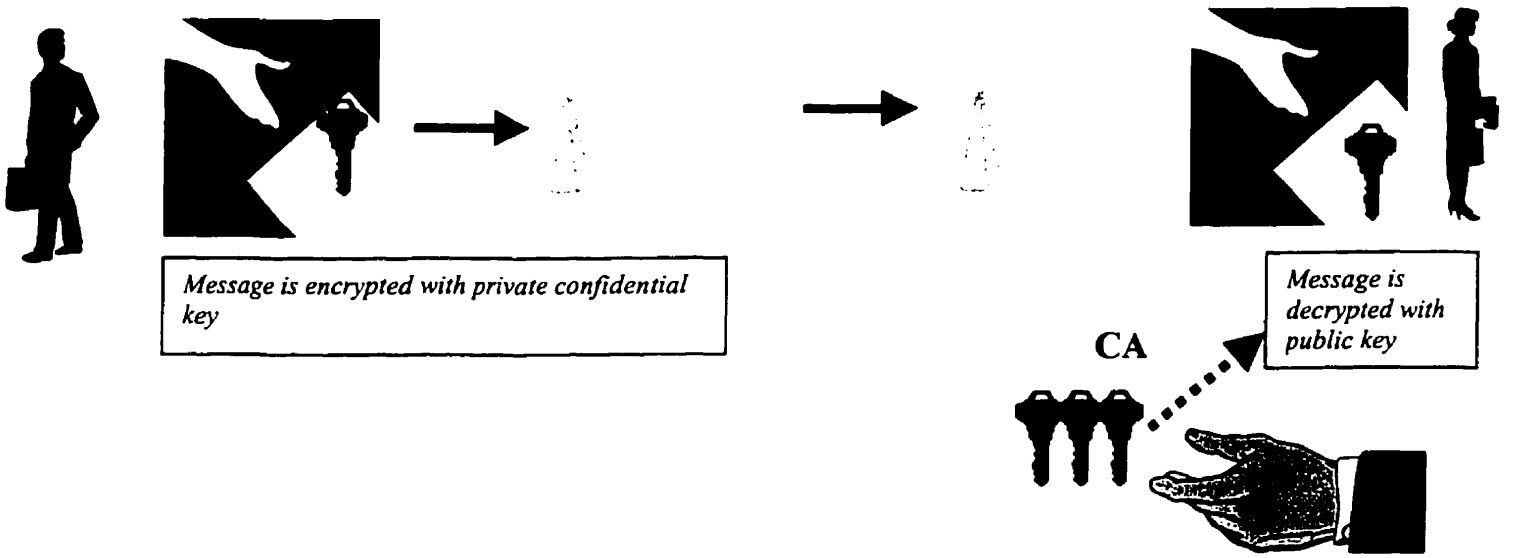
[61] R.H Baker, *Network security: how to plan for it and achieve it*, I ed. (New York: McGraw-Hill , 1995) at 143 See also *Menezes supra* note 36

[62] *Supra* note *54* at 306

An example of how public key encryption works

Example 1.

Bob wants to send an encrypted message to Alice. Bob encrypts the message using his private key before transmitting it. Alice can decrypt the message by using Bob's public key that he has distributed to Alice. Alice knows that Bob sent the message because only Bob could have encrypted it. Bob cannot disavow the message's authenticity, therefore the entire message serves as a signature. The message is authenticated and verified because the message could not have been altered without access to Bob's private key. The disadvantage of encrypting the entire message is that it takes more time to encrypt and decrypt it. Moreover, it requires a great deal of storage capacity. A law firm for example would most certainly have to keep one copy of the message in plaintext and one ciphered message with which to verify the plaintext message.[63] Another method, which is faster, is therefore to only encrypt (seal) the most important part of the message. The minimum portion of the message should include; the receiver's name the transmitter's name, a checksum and a sequence number. This portion of the message is the digital signature that verifies its origin, content and sequence.

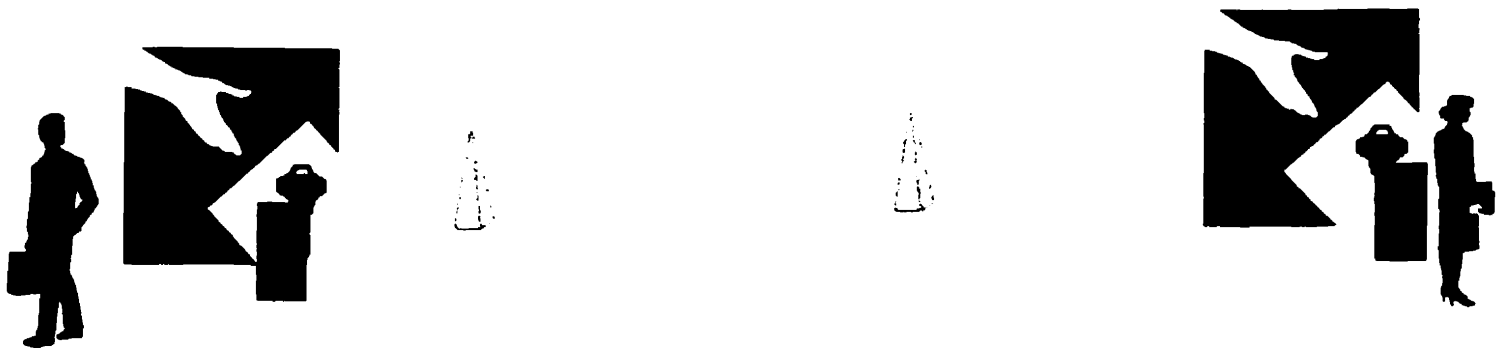


[63] The ciphered message might be lost or altered in any way. If the decryption key is lost it is vital to at least have a hard copy.

If Bob wants to ensure that Alice and only Alice can read the message he has to encrypt the message once more using Alice's public key.

Example 2.

Bob begins the same way by encrypting the message using his private key. By doing so he is assured that only someone holding his public key can decrypt the message. Now he wants to ensure that only Alice can read the message. He therefore uses Alice's public key to encrypt the message once more. Only Alice holds the corresponding private key and she is therefore the only one who can decipher that layer of encryption. The disadvantage of this method is that the message needs to be encrypted and decrypted four times.



Requirements for a public key system

The problem with a public key system is, as always when human beings are involved, key management. Public key systems assume that the private key has not been compromised. Everyone knows how difficult it is to keep track of all the pin codes that we use in our daily life. We need pin codes to identify ourselves in many ways: to get through doors, to get access to computers and to withdraw money from our bank accounts just to mention a few examples. We can assume that private keys will be compromised eventually and we have to create a system that deals with it in a coherent fashion. A public key system, furthermore, assumes that the recipient always has a valid

copy of the sender's public key. Can the key be trusted? If somebody falsely alleges that a public key belongs to a person, then a valid signature could be forged.
Example: Person A distributes a public key to B and claims it belongs to C. (In reality C has another public key.) B accepts a contract that he assumes comes from C and sends a message with his acceptance to whom he thinks is C. A decrypts the message with the corresponding private key and urges B to pay promptly to a bank account, which is not C's but in fact A's. This example illustrates the problem with trust in a networked world with anonymous parties.[64]

Considerations that should be made when choosing a cryptographic system

Which encryption method a user shall chose heavily depends on the length of the message, the desired security level and the desired encryption speed. A method that avoids encryption of the whole or part of the message might have several advantages. If no encryption is used less computing power is needed because encryption has not to be performed for every message, however small or insignificant, that passes to the gateway to the network. Hardware encryption is, moreover, designed for large blocks of data. In most cases hardware has to be used to provide real-time encryption.[65] If the messages usually sent are small a large proportion of the time will be spent on initializing and invocation making the process wasteful and time consuming. Most of the encryption algorithms, such as the RSA public key algorithm, are moreover patented. The user therefore has to pay a fee to the patent holder or patent holders, which will add extra cost. Strong encryption algorithms exceeding certain key lengths are furthermore subject to export control in the USA for example. This means that either a license has to be obtained or that certain export requirements might have to be fulfilled by the user.

User identification

To prevent unauthorized access to computer systems passwords are used. Security can be further increased if a password is used in conjunction with some other kind of

[64] Several methods of how to organize key management have been suggested. The X.509 standard that seems to be winning the greatest international acceptance has been criticized as being to unwieldy See for example S. Handa et al, "Re-Evaluating Proposals for a Public Key Infrastructure", online http://www.law.mcgill.ca/coursenotes/complaw/papers/1995-pki.htm (date accessed: 10 October 1997)
[65] *Supra* Hyatt note 57 at 314

identification system, such as a magnetic stripe card, or a smart card. The information stored in the computer to verify the passwords should of course be encrypted.[66]

Non-repudiation

The cryptographic possibility of non-repudiation in an asymmetric cryptosystem can be used to prevent impersonation and denial of creation.[67] The creator (sender) cannot deny creating a message because it is presumed that only he had access to the used private key with which the message was enciphered. Non-repudiation is, however, only possible in an asymmetric system because in such a system the keys are not the same. If A and B share the same key, B can forge a message and allege it comes from A. The possibility of providing for non-repudiation in asymmetric cryptographic systems stems from the use of a digital signature to create a digest of a message to produce a hash. The hash is based on information about the sender and the digest of the message. A document signed with a digital signature will assure the receiver who the sender is, because that person and only that person is presumed to have access to the private signature key i.e. the usage of that key confirms and verifies the sender. The receiver can, furthermore, be assured that the message received was the message actually sent and not another one it has been replaced with, i.e. proof of the identity of the message. A digital signature can, moreover, include a date, time and sequence stamp.(It is actually not a stamp, but something quite comparable- encrypted data- which makes it non-removable unless you are in the possession of the encryption key.)[68]
The underlying presumption that only the rightful owner will have had access to the key underlies most authorization schemes, although we do not always think about it. We

[66] It should be remembered that no chain will be stronger than its weakest link. If strong encryption is used the codebreakers will focus on the operating system instead. Since an increasing number of people are using modems to get access to the Internet and very few of those are using any preventive measures at all the use of strong encryption might mislead the user to think that he is well protected. Getting so called root access to a computer through a modem is not very difficult for a determined hacker. There even exist programs as such as e.g. Netbus to facilitate these kind of activities.
[67] Kenneth W. Dam , *Cryptography's Role in Securing the Information Society*, (National Research Council, Computer and Telecommunication Board) (Washington DC: National Academy of Sciences, National Academy Press, 1996) at 370
[68] The safest and most trustworthy method is to let a third party certify the creation of a document and date/time stamp it. *Ibid Crisis* at 371 and B. Cipra, *Electronic Time-Stamping: The Notary Public Goes Digital*, Science (1993), Volume 261 (5118), 9 July 1993 at 162-163, available online at: Science http://www.surety.com

assume for example that only Bob has that voice and only Alice has that signature. The underlying presumption in a digital signature scheme is in fact more trustworthy, because it is mathematically infeasible that anyone has an identical key, while it is not impossible that two persons have similar voices or handwriting.[69]

Confidentiality

It is important to distinguish between cryptography used for confidentiality and cryptography used for other purposes such as authentication. Only cryptography used for confidentiality purposes possesses a threat to law-enforcement and national security. Authentication will in fact enhance secure transactions and prevent e.g. fraud. A loss of a private signature key is *per se* more serious than losing a private key for encryption since the loss of a private signature key may lead to wrongful implication of the rightful holder of the key.

The need for encryption for confidentiality depends, besides the value of the information and the sensitivity of the information, on the medium used for communication. We have in the last two years seen an explosion of mobile telecommunication and of voice telephony over the Internet, which until now have offered very little protection against interception.[70]

Integrity of data

All information can be stored as 0 or 1; this is called a binary system. It is important to be able to control that sent data has not been altered in any way. The reason for this is rather evident since the data might be either unreadable or incorrect. If the data is unreadable it is obvious to the receiver that something has happened and that the received information cannot be trusted. It is much worse if data has been altered in a way that is not easily detectable. Error-control of data is usually done when data is transmitted by different protocols.[71] The error-controls are, however, sent openly with

[69] On the other hand a specific voice is a hereditary characteristic that cannot be lost. A private signature key can be lost unknowingly.

[70] Modern GSM-nets are encrypted in for example Sweden between the mobile telephone and the base station. Older analog mobile telephones are however not encrypted.

[71] Various error-correcting codes can be used, for example parity-checks or cyclic redundancy checks. See further *Crisis Supra* note 67 at 366.

the message and can therefore be manipulated to cohere with the altered message. Cryptographic integrity controls are different in this respect as a cryptographic integrity check is tamper resistant and secret for all but the intended receiver.[72]

Alteration

It is of essential interest for e-commerce on the Internet that a message reaches the receiver in its original form. Alteration can be divided into two types; unintentional and intentional. The most dangerous form of alteration is intentional and malicious. If a party to a contract intentionally changes the contract sum in an electronic contract from 200,000 to 2,000,000 then the paying party might have problem proving that the contract has been altered since it is in electronic form. In the electronic world no original exists and, furthermore, the burden of proof usually rests on the party claiming that a contract has been altered. Unintentional alteration might be as serious as intentional, depending on the form of the alteration and whether the alteration can be detected easily. A power failure during the transmission of a contact, which results in an unreadable output, is usually not very serious because it is easily detected. As explained under the headline Authentication, alteration is merely the other side of the coin of authentication.

One method of ensuring that a message or a contract has not been altered is hashing.[73] By transforming a message into numbers and calculating the result to get a sum, one obtains a value that can be used to verify that a message has not been altered. This checksum, represented by a set of numbers, is unique to the message and is sent with the message. If the receiving computer, using the same mathematical algorithm, does not reach the same result (the same checksum) one can conclude that the message has been altered.

Integrity of data in a symmetric key system

In a symmetric key system only the sender and the receiver are supposed to be in possession of the key, so no malicious attempts to alter the data can be made. The

[72] An integrity check is sometimes called a message authenticator and is usually a cryptographic checksum.

receiver will, however, only be able to notice if the message has been altered by the other party if the text has been signed digitally by a third party. He can then compare the encrypted values and detect if the text has been altered. It is important to stress that a symmetric cryptographic system presupposes that the parties trust each other.

Integrity in an asymmetric cryptosystem

Usually a one-way hash function is used in an asymmetric cryptosystem.[74]The word one-way indicates that it is easy to compute the hash, but computationally infeasible to deduce the plaintext of the hash. The hash value is signed by the private signature key to produce a digital signature.

2.2.2. Attacks on cryptographic systems

Cryptographic systems may either be open or secret. Military cryptographic systems are usually secret. The purpose of keeping an algorithm secret is to keep cryptographic research of what constitutes a good cryptographic algorithm out of the public domain, and, moreover, to prevent cryptoanalysts from exploring weaknesses of the algorithm.[75] The advantage of keeping an algorithm open is to render it possible to evaluate the algorithm. The security in an open cryptographic system depends foremost on the key and not on keeping the algorithm itself secret. If the algorithm is kept secret then the users have to trust the integrity of the algorithm and its developer and that no "backdoors" are built into the algorithm.

An algorithm for military usage is used within the same organization and trust between the parties is therefore taken for granted. On the other hand in the open commercial market the developer or manufacturer has to establish trust from the potential buyer. The civilian user is presumably going to use the cryptographic product for sensitive information and the concept of trust is therefore essential for the user. A customer will not use an algorithm that he does not trust completely. An algorithm developed on the open market may be used by several organizations and users that are both competing and cooperating with each other. The level of security therefore lies not

---

[73] D. Johnston, S. Handa, C. Morgan, *Cyberlaw: What you need to do business online*, 1st ed.(Toronto: Stoddart 1997) at 90

[74] See *Crisis supra* note 67 at 37

in the secrecy of an algorithm, but in a thoroughly publicly tested algorithm and a complex key that is not easily broken by a brute-force attack.[76] When discussing attacks on cryptographic systems it is important to stress that cryptographic systems are secure subject to certain prerequisites, for example that the one-time pads are used only once. Provided that the same pair of one-time pads are used only once the system is theoretically unbreakable. History shows, however, that people make mistakes and cryptoanalysts who try to break a cryptographic system of course try to find the easiest way to break the cryptographic system and take advantage of sloppy procedures.[77]

Whether a cryptographic system is possible to break is very much dependent on the resources at the attacker's disposal. Only a few governments have the financial resources, time, computing power and cryptographic expertise needed to break more complex cryptographic systems. Security is therefore a trade off between the value of the information and the cost of implementing a system in order to have an appropriate security level.[78] The difficulty in breaking a cryptosystem is generally dependent on the strength of the algorithm and the key length.[79] With a sufficient key size a brute force attack is unfeasible.[80] However, there is also a relation between key size and speed. Some cryptographic systems utilizing keys over a certain key length are not suitable for real time communication because they are too slow.

Bruteforce attacks

One technique to break an encryption scheme previously mentioned is to use a brute-force search.[81] If a crypotanalyst finds a sample of plaintext (a text that has not been

---

[75] *Ibid* at 384

[76] Several cryptographic researchers criticized the Clipper chip as unsecure because NSA had not disclosed the algorithm. The algorithm could therefore not be tested and analyzed. There was no possibility to assess if any backdoors had been built in. (A bruteforce attack is an exhaustion attack in which all possible keys are tested.)

[77] The Soviet Union earlier used one-time pads to protect diplomatic communication. A mistake was however made and some one-time pads were used more than once, thereby enabling cryptoanalysts to break messages. See further G. Johnson, "The spies, Code and how it broke", *New York Times: Week in review*, 16 July, 1995 at 4. See also *Privacy on the line* at 19 and "The Verona Project" (1997), online : http://www.nsa.gov:8080/docs/verona/ddir.html (date accessed: 22 July 1998)

[78] The possibility to use strong cryptographic systems might have come to change this since affordable unbreakable security is available to all computer users.

[79] A certain key length is mostly relevant for symmetric cryptographic systems.

[80] *Supra* note 67 at 379.

[81] *Supra* note 31 at 50

ciphered) and the corresponding ciphertext but does not have the key, then he can execute a brute-force search by trying every possible key.

Example: If f(x)=y and you know y (a plaintext value (letter)) and f then you can find x by trying every possible y.

In the end the ciphertext and the plaintext will match and you can read the message. However, every well-designed encryption system such as the DES (Digital Encryption Standard) has such a large key range of possible keys as to make brute-force attacks impractical.[82] The DES has for example 2^{56} possible keys. Brute force attacks are thus very much dependent on computing power. Computer chips are on the other hand becoming faster and faster. At the same time as the price of computer chips drops, CPU speed is also increasing. These two factors together with intensive research in cryptoanalysis makes brute force attacks more probable, but not by necessarily successful, since it is possible to further enlarge the key space apace.

Attacks against protocols

Attacks against cryptographic systems can be divided into active and passive attacks depending on the purpose of the attack.[83] In the event the purpose is only to listen into a communication it is called a passive attack. These attacks are hard to detect because there are no changes to the protocol that can be observed and the best protections are therefore preventive measures. The active attack involves some kind of active intervention with the function of the protocol. The active attacker may for example try to alter the protocol to his own advantage or to delete sent information.

[82] In 1995 a person posted a news article to the hacker community claiming that he had decrypted a message by breaking a RC4 algorithm with a 40-bit key. He used 120 workstations and 2 parallel supercomputers at three major research centers for eight days to break the cipher. *Supra* Digital Cash note 31 at 58. As this chestnut illustrates breaking an encryption code is a question of money, computing power and time.

[83] Applied cryptography *Supra* note 46 at 26

2.2.3 Trust in Cryptographic Systems

Key security

The strength of a cryptographic system depends on primarily two things; the algorithm and the length of the key.[84] The security provided by the key varies depending on the type of cryptographic system and will vary for symmetric and asymmetric cryptography. The reason why keys should not be longer than necessary is, of course, that long keys slow down the encipher/decipher process. Therefore, the key should be no longer than required to achieve the necessary level of security for the information.[85]

Preferred length for symmetric key systems

As described earlier, cryptographic algorithms for the commercial market are usually publicly known and tested. If the algorithm does not have any considerable weaknesses the only alternative means of breaking the crypto is to launch a brute force attack, i.e. to try every possible key. This is known as a *known-plaintext attack.* Once the cryptoanalyst has got a piece of the plaintext and the corresponding ciphertext he can proceed with the attack. There are a number of ways the cryptoanalyst can obtain the ciphertext and plaintext. If he knows the format of the file he can automatically deduce some plaintext because the format is standardized and messages usually start in the same formal way. The chance of finding the correct key in a symmetric cryptosystem depends on the length of the key. If the key for example is 8 bits long there are $2^8 = 256$ possible keys. Statistically there is a 50% chance to find the key after half of the attempts.

The number of keys that can be calculated per second depends on the speed of the computer.[86] Computers can be built specifically to break cryptosystems and the time

---

[84] *Ibid* at 151

[85] See Computer Security and the Data Encryption Standard *Supra note* 35 at 9 and Applied cryptography *Supra* note 46 at 167

[86] The speed with which the keys can be tested depends very much on the algorithm, but the algorithm is not the most important when it comes to speed. Special parallel machines can be constructed to try keys and the key space can be divided and tried separately by processors. The price/speed ratio for breaking the DES is linear and a machine capable of breaking the DES in an average of 3.5 hours could in 1995 be built for $1 million. A cost, which might be acceptable, considered the large huge amounts of money being transferred by the DES. Moore's law, that earlier stated that computing power doubles every 18 months had recently been revised (See note 11) According to Moore's law computing power currently

required can thus be reduced. With e.g. a key length of 56 bits (as in the case of the DES) and a computer capable of trying a million keys a second it would take 10^{25} years to try all possible keys.[87] The universe, by comparison, is only 10^{10} years old. The speed at which the key can be tested depends on whether code-breaking machines can be built to break the cryptographic system or a software attack has to be launched. A software attack is usually about 1000 times slower. On the other hand networks can be connected to each other and considerable computing power may therefore be accessible at the same time.

Length of keys in public key systems

The security of a public key system is usually based on the mathematical difficulty of factoring large numbers that are the product of two prime numbers or of solving discrete logarithm problems. The difficulty of breaking an algorithm is in trying to factor either the large prime number or, in the case of a discrete logarithm problem, to calculate discrete logarithms in a very large but finite field.[88] When calculating the required length of public-key-systems the unit million instructions per second is used. A Pentium 100 MHz microprocessor is capable of 50 mips (one-million-instructions-per-second). To factor a number with 2048 bits will take $3x10^{20}$ mips years and therefore should represent sufficient key length to last 30 years, even though predictions about development in mathematics and technology are always hard to make.[89]

Key escrow

For key escrow to be internationally accepted cooperation over national boundaries will be necessary. Perhaps some kind of supranational organization needs to be established to take care of key management. However, such an idea would almost certainly be

---

doubles every 9 months. The fast development will make it considerable cheaper to build a code breaking machine for every year that passes. See further Applied cryptography *Supra* note 46 at 153 and W. Diffie and M.E. Hellman, "Exhaustive Cryptoanalysis of the NBS Data Encryption Standard", Jun 1977, v.10, n. 6, Computers, at 74 ff See also for more information M.J. Wiener, "Efficient DES Key Search" presented at the CRYPTO rump session in August 1993, TR-244, School of Computer Science, Carleton University, May 1994

[87] See Applied Cryptography *Supra* note 46 at 152.

[88] *Ibid* at 158

[89] *Ibid* at 161

rejected by several countries. One need only study the development of the European Union to see the difficulties in creating supranational organizations. Even though the European Union is a major step towards economic integration, issues such as national security have been excluded. The establishment of a common currency has also been preceded by years of discussions and arguments over issues such as national sovereignty. Some countries even opted out because of fear of loss of national sovereignty.[90] For these reasons it is hard to believe that many states should agree to create a supranational key management infrastructure where keys were held in escrow.

[90] In for example Sweden one of the arguments heard in the public debate was that Sweden would have to give up sovereignty and would not have a possibility to e.g. devaluate.

PART III: Societal gain of encryption

I will below try to give some background to some of the greatest forces behind cryptography and why cryptography will be important in the future.

3.1 Electronic Commerce

Electronic commerce enhances a wide spectrum of business activities, such as contracting electronically, electronic information services and electronic payment systems. Electronic commerce will probably make the market more global than it is today. Even though we have had an international market before, the new market created by electronic commerce will be between smaller entities and consumers that are not accustomed to international transactions. The entities and consumers are also far more anonymous to each other. An early form of electronic commerce, Electronic Data Interchange (EDI) has been used between large entities for about two decades and continues to grow.[91] It is believed that electronic commerce will grow stronger in business to business commerce in comparison to direct-to-consumer commerce.[92] Today an increasing number of mail orders are being made through the Internet. According to a report in 1998 by the Boston Consulting Group, online retailing would generate more than USD 36 billion 1999, which is almost double the revenue in 1998, USD 14.9 billion.[93] In the USA, 53 percent of the Internet consumers had made an online purchase in 1999, spending an average of USD 206 per purchase. 35 percent of these consumers purchased less from offline stores and 38 percent less from mailorder catalogues according to the survey. Of those surveyed, 36 percent expressed concern

[91] EDI (Electronic Data Interchange) is a form of electronic contracting. By determining certain parameters beforehand electronic contracts are concluded without human interaction.

[92] According to a study by Peppers and Rogers Group the number of households using Consumer Direct (CD) e-commerce and grocery delivery services, will grow from 6 million households in 1999 to 29 million households in 2010. CD sales will year 2010 account for almost 10 percent of all retail sales. Direct to consumer sales are expected to generate up to USD 1.1 trillion 2010 compared to 190 billion in 1998. For more information see "Shopping behavior in the age of interactivity" (1 July 1999) online: http://www.1to1.com/articles/i1-070199/cdirect.html, (date accessed: 24 July 1999)

[93] See "Shop.org: Online retailing to Top USD 36 Billion in 1999", online: http://www.nua.ie/surveys/index.cgi?f=VS&art_id=90535503&rel=true, (date accessed: 22 July 1999)

about security of shopping online.[94] Electronic Commerce offers many advantages over traditional transactions. The customer can sit at home and choose what he wants to buy at times that are convenient to him and he can place an order immediately if he so pleases.[95]

For business Electronic Commerce also has many advantages. A company does e.g. not have to have hire as many salespersons, marketing cost are much lower and the investment set-up cost are considerably lower, to mention a few examples. This makes it easier for small business enterprises to enter new sectors and enables them to compete with traditional larger companies. In particular small companies with narrow product ranges have access to a wider customer base .

Three elements are critical for electronic commerce; delivery systems, payment systems and authorization systems. Delivery systems have emerged especially for information services and intellectual property. One example of information services is the blue flag, a provider of legal services through the Internet. Another example is electronic tickets that are being issued by Air Canada and Scandinavian Airline Systems (SAS). Cryptography can also be used to authorize release of information and to authenticate the information provided.

Closely connected to delivery is payment for goods and services. A number of standards have emerged, for example the SET standard. No standard has, however, yet become dominant. Payment systems can roughly be divided into two general groups: payment mechanisms related to a contractual relationship e.g. a credit card company or a bank on one hand and electronic cash (e-money and cybercash are some brand names that have emerged) on the other hand.

In order for electronic payment systems to become an alternative to the current payment systems they have to be fast, inexpensive and internationally recognized. A

---

[94] See "Navidec Inc: 53 percent of US Users Have Bought Online", online: http://www.nua.ie/surveys/index.cgi?VS&art_id=905355027&rel=true, (date accessed: 22 July 1999) The survey was based on a telephone survey with 1, 000 US Internet users. I must say that I question the figures somewhat and I wonder how the customers were selected. If they were selected based on previous online consuming the survey is not interesting.

[95] To what extent the customer is protected when he order things over the Internet is still unclear. The Rome convention regulates choice of law when a cross-border transaction is done and the Lugano convention regulates forum. The Lugano convention gives the customer a certain protection because a customer can only be summoned in his home country while the customer has the choice to summon the manufacturer either in his home country or in the manufacturer's home country.

system for satisfying liabilities, especially liability in international transactions, has to be established. Cryptography is used in many ways to enhance these transactions. Authorization is an important area closely related with many other elements of a transaction. The buyer needs for example to know from whom he is buying, in order to know if the products are authentic and to avoid being defrauded. In an electronic world the different parties will become more anonymous to each other. Mechanisms such as digital signatures are therefore necessary.[96] One of the stumbling blocks of electronic commerce is security, especially in larger transactions.

Electronic commerce is expected to start growing rapidly as soon as the problem of transaction security has been solved. It is therefore important to reach an international consensus regarding the use and export of cryptography.

3.2 Intellectual Property

An important and growing application for cryptography is protection of intellectual property rights. The development of computers has opened up new possibilities for creators and authors. The development of digital technology, widespread use of computers and progress in telecommunication technology has, moreover, resulted in works being able to be copied and spread more easily than ever. Even though strong intellectual property laws exist they are not always respected. Creators of works have very little ability to ensure that their works are not being copied once they have been put on the market. Cryptography potentially enable authors to make it more difficult for others to copy their work and at the same time allows them to detect illegal copies more easily. Cryptography can thereby help enforce intellectual property laws and help the creator or inventor to distribute and control legally made copies. Encrypting the information in files stored, for example, on CD-ROMS can serve as a protection against illegal copying. To open a file the individual key relating to that file is needed. In order to identify individual copies cryptographic algorithms can be used to tag data for identification purposes.

---

[96] The authorization does not have to be related to an actual person. It is usually enough if for example the seller knows that the buyer has enough funds when he is using a credit card. Use of authorization schemes raises privacy questions since the digital buyer leaves traces which can be compiled and which create a very detailed picture of a buyer and his private interests.

A market segment where encryption has been used for some time is satellite and cable television. A satellite channel can usually only be accessed if the potential viewer has a smartcard with the decryption keys. When the viewer wants to watch e.g. a pay-per-view film offered by a cable company the cable company has to send an unlocking signal first to unlock the film.[97] In order to trace copies either the copy is individualized or attributed to the buyer. However, the last alternative raises privacy concerns.

3.3 Electronic Payment systems

Electronic payment systems can be divided into either account based payment mechanisms or electronic cash. Electronic cash brings new technical and legal challenges to make transactions secure.

One area where global access to strong encryption will be necessary is that of electronic cash. The paper money systems currently used are quite expensive to operate, largely because of the security risks that are involved in cash transactions. Security always costs money, in one or another way. In order for electronic money systems to work, the systems has to be very safe, trusted and widely used. Electronic cash is usually in the form of either tokens or value stored on smart cards. The electronic tokens used are basically an encrypted electronic record representing a value fixed to a currency. When an electronic purchase is made the electronic token is passed over to the trader who then cashes the token with a bank. If a smart card is being used, for example the Mondex smartcard, no involvement of a third party is necessary since money can be passed direct from one card to another card. The smartcard contains electronic tokens originally purchased through a financial institution such as a bank. When a purchase is made the electronic record is passed over directly to the other card. The benefit or disadvantage, depending on your perspective, with the Mondex card is that it more closely resembles real money, thereby offering the parties greater privacy. For the money launderer it offers the possibility to transfer large amounts of close-to-cash funds without leaving any digital traces. Carrying large amounts of real cash always involves a risk. Using Mondex cards reduces this risk but retains the traditional features of cash.

---

[97] P. Wayner, *Digital Copyright Protection* (New York: AP Professional, 1997) at 3. [hereinafter *Wayner*]

3.4 Digital signatures

Digital signatures are an important part of the infrastructure of electronic commerce. In an electronic commerce context is it essential to be able to verify the true identity of the digital signature owner. That an irrevocable digital signature has been created with a certain signature key is easy to establish. The legal identity of the key holder is, however, more difficult to verify. The danger of impersonation by assuming someone else's identity is obvious, especially in the relatively anonymous electronic environment.

The holder of a digital signature is presumed to have a legal capacity to sign a contract. To take an example: a person called A alleges he is person B and publishes a digital signature key that is created by A but which A alleges belongs to B. A might then perhaps be able to receive payment to B, because there is an underlying presumption that two identical private key pairs do not exist. We can therefore establish that there is a need to be sure that an individual person or an entity with a pair of digital signature keys really is the one that he or she alleges to be. This can be achieved in several ways, either laterally by letting the users certify each other thereby creating a web of trust, or vertically by creating some kind of certification authority (CA). CAs, or Trusted Third Parties (TTPs) as they sometimes are called, can be used in a key recovery program or in a key escrow program. This is one aspect that links cryptography for confidentiality with cryptography for authentication.

3.5 Privacy[98]

Debate about privacy questions ensued when computers became more widespread in the 1960s. Since then the debate has been going on. Privacy issues are closely related to the use of computers since computers make it easy to compile records. Information becomes more and more significant and valuable. The use of cryptography may, however, offer a possibility to win back some of the ground lost over the years. David Chaum wrote already ten years ago:

> " Soon, by accessing a computerized network from almost anywhere, you may be able to pay for a purchase, order a film to be shown in your home, change your

[98] This part describes privacy and implications for privacy more generally. The work in the OECD with relation to privacy is further described and analyzed in part IV under the OECD Cryptography Policy Guidelines. Principle number five in the guidelines concerns protection of privacy and personal data.

> life insurance policy, or perhaps send an electronic "letter" to a friend...This current approach requires individuals to identify themselves to the system every time they use it. All the various identifying techniques –like current plastic cards, memorized secret numbers, and fingerprints-are essentially equivalent to universal ID numbers, such as the ones used for social insurance and passports. These identifiers allow computerized linking of financial, employment, medical, and all manners of other personal data, laying bare individuals' lives to an unprecedented extent. Moreover, longstanding fears of Big Brother are being given new legitimacy by advances in "automatic pattern recognition". With these system anyone tapping into the large-scale systems currently being planned could automatically categorize individuals by their transaction patterns- everywhere they pay, what organizations they have relationships with, and who they communicate with –in the form of invisible mass surveillance. Legal mechanisms, faced with the ease of tapping and modifying computerized data, seem powerless to avert such dangers or to protect individuals from the resulting potential for errors and discrimination."[99]

We are indeed in the society described by David Chaum now. We have networks of networks of computers, the Internet, e-mail and webtv. Little has, however, been done to protect customers from data mining.[100] One solution suggested by David Chaum was unconditionally untraceable electronic money. The risk involved with untraceable money is that it can be used for money laundering. How to balance between protecting privacy and the risk of money laundering is up to the legislator. There is, however, in my belief, a larger risk for the society from not legislating at all to protect privacy. If the public does not feel that their fear and concerns are taken seriously they will demand untraceable transactions, which might not be in the government's interest. If it is up to the individual businesses themselves to regulate how information is gathered and if businesses are not able to live up to the expectations of the broader public, then the public will start demanding untraceable electronic cash and strong encryption to protect their privacy. The current wait-and-see policy by many governments may therefore backfire. If governments do not make timely policy statements and legislation in time they will probably have to regulate much more rigorously eventually. The public will then definitely feel as if the government is interfering unduly. To what extent the present self-regulation of privacy will work remains to be evaluated. So far it has not

[99] Brassard *Supra* note 10 at 70

worked very well. One reason why self-regulation has not worked is that financial institutions are making money by selling information. The regulation of a lucrative business is therefore not in their interest. The customer himself does not have enough authority to be able to dictate more favorable contract conditions regarding privacy issues. Furthermore, once an individual has signed a contract he has very little control over the information supplied for the contract. If for example a customer wants to purchase a Walkman on the Internet he has to become a member of the website first and give out a substantial amount of personal information about income and the household.

A way for the individual to retain control over information has been suggested by Gilles Brassard.[101] He suggests credentials may be established by means of having personal information encrypted on cards issued by independent organizations. The credentials as well as other information on the card is stored as coded non-forgeable signatures. A financial institution asking information about you can therefore request information from yourself and receive reliable information about your financial situation because the information is encrypted and tamperproof. The financial institution is receiving a restricted range of specific information. What information is released is up to the cardholder. The information is never being transmitted without the cardholder's permission and stays within the cardholder's control.

We might have reached a point where public confidence in privacy protection has reached a low-level mark. More and more users will resort to cryptography to protect their privacy. Awareness of privacy problems from a political point of view is not the issue. The problem lies in the implementation of legislative guidelines and codes of conduct. The results of the ineffectiveness and the futility of sanctions can be severe. Firstly, information about consumers and their buying behavior has a value, which means that the use of personal data needs to be restricted. Secondly, data and information is usually not traceable once put into circulation. An individual has no or very little means of controlling for example information that he has provided on a website.

---

[100] The European Union has reached considerably further than the U.S.A. and Canada in this respect. It seems to me that privacy laws within the European Union are more focused on individual privacy contra commercial interests rather than government intrusion.

[101] Brassard, *supra* note 10 at 72

In 1988 David Chaum thought that we were fast approaching a moment of crucial and irreversible decision, not only between transaction systems but also between two kinds of society.[102]

> "If the current trend continues, the enormous surveillance potential of such automated systems will not only render hollow most legal safeguards on privacy and other protections, but may seriously chill participation in public and political life. If, on the other hand, the new approach prevails, erosion of individuals' rights can be reversed and new rights added—notably the right, made possible by personal card computers, to reveal only necessary information in transactions. In an age of persuasive computerization, control over information is the key to social and economic and political power."

Regulation, however, might not be the best way to solve the problem. When privacy is not protected to the extent people think it should be, they try to resolve the problem by other means and one of these means is encryption. Encryption provides individuals with a tool to protect the privacy they feel they need. Nobody would consider it fair to open and read somebody else's letters. However, in a business organization it is not considered as a violation of the individual's privacy if the employer reads the employees e-mail. The use of strong encryption will make it difficult not only for law-enforcement agencies to act against criminal activities, but also make it hard for employers to monitor their employees. The employers' action will probably be to prohibit employees from using encryption unless duly authorized. Employees will on the other hand see this as a violation of their freedom of speech. Companies might, furthermore, want to control aspects of information they provide to their employees. If the employees are using cryptography the employer might want to have the private keys. Companies may also be afraid that an employee might encrypt information on the network if he is fired. It all comes down to trust.

We definitely need some checks and balances as Montesquieu stated in his famous book *the Spirit of Laws* in 1600.[103] We do not either want to have the kind of society George Orwell described in his book *1984*. The question is if we can live in a society where no-one trusts anyone else? Without a doubt protection of privacy has become one of the most important issues in the debate over the Internet and open

---

[102] Brassard, *Ibid* note 10 at 71

[103] According to Montesquieu governmental powers should be separated and balanced to guarantee individual rights and freedom.

networks. The first threat for individual privacy emerged with the computerization, when computer files could easily be compiled, linked and matched. This had the result that even small fragments of personal information could become threats to privacy when they were compiled. The second threat is emerging now when all networks are connected together and individuals to a great extent have lost control over personal information released about themselves. People neither know what kind of information about them that exists, nor have they any possibility of correcting incorrect information.

PART IV: Possible consequences and implications for law enforcement agencies and national security agencies that encryption might have

4.1. Law enforcement

The main reason why strong encryption has not been permitted so far worldwide is the fear of extensive criminal abuse of encryption. Encryption would make it very hard for law enforcement agencies to gather information when conducting searches and seizures of information stored as encrypted data. A result of frequent use of encryption is that encrypted information or transmissions will no longer stand out in the information flow, which will make it difficult to conduct traffic analysis. Until now the use of encryption has interested law enforcement agencies as well as national security agencies because use of encryption programs suggests that the sender has something to hide. When almost all information is encrypted national security agencies and law enforcement agencies will no longer have resources enough to eavesdrop on all traffic. Successfully combating crime today involves heavy use of electronic surveillance in different forms. Use of strong encryption will limit these possibilities. On the other hand strong encryption has already become widespread and is in any case probably already in the hands of the criminal organizations that want to use strong encryption. If these organizations do not have it yet they are at least able to obtain it rather easily.

4.2 National security interests

Closely related to law enforcement objectives are national security interests. It is likely that national security interests rather than law enforcement objectives are the main reason for proposals regarding mandatory key recovery or key escrow systems. The U.S.A. has constantly developed their intelligence systems and has therefore a lot to lose in terms of intelligence capability. Today access to information is essential for governments. If encryption becomes widespread it might deprive the U.S. intelligence services one of their biggest advantages. The U.S intelligence system that has been built over the last three decades has cost billions of dollars and the U.S. Government therefore has a strong incentive to retain the status quo. Not surprisingly the USA has also been one of the loudest advocates for key recovery and key escrow.

Intelligence and Counterintelligence

One of the areas, in which cryptography is essential, is that of national security purposes. Cryptography has always been closely related to national intelligence and counterintelligence. It is therefore necessary to have a brief understanding of national intelligence agencies and their work. We are no longer moving into the information society-we are already there. Vital national interests are highly dependent on computers and networks and so are the armed forces. Information has, moreover, become increasingly important on the battlefield, as well as in the political and economic arena. Therefore intelligence resources are becoming increasingly important. Today sophisticated information technology dominates the battlefield. Sophisticated information systems for surveillance and interception of telecommunications does however pose a threat to individual privacy.

Intelligence work is an area surrounded by secrecy. It is, moreover, an area that has changed considerably over the last decades due to political occurrences, such as the fall of the Soviet Union and technological developments. Although it is difficult to get a full picture of the scope and extent of any country's intelligence scope and methods, because of the confidential nature of intelligence gathering, is it important to have an understanding of how intelligence is collected and for what purposes. One argument raised against the use of strong encryption is that it would seriously impede legitimate work by law enforcement agencies and national security agencies. To be able to evaluate the validity of those arguments it is necessary to have a background to intelligence gathering in the 20th century. The most developed country in this respect is undoubtedly the USA who has spent a considerable effort to become a world leader in this arena. Most of the examples and the information below refer to the USA, but parallels can be drawn with other countries' intelligence services as well.

A Background to Intelligence Issues [104]

In an intelligence mission many different sources are used to verify each other. Several different sources indicating the same information make the original indication more

[104] Information below, unless otherwise indicated, are gathered from the Crisis report *supra* note 67 at 421-429.

reliable. Even though a majority of intelligence sources are clandestine, more and more information can be collected from public databases. The Internet for example contains a vast amount of information and, thanks to increasingly refined search engines, often specialized for intelligence work, more and more information can be gathered and compiled from public sources.[105] However, clandestine sources and Human Intelligence (Humint) are still critical and will probably remain essential for intelligence work in the future.

Intelligence can be defined as the synthesis of information from all possible sources and is pursued on a level-of-effort basis. Accessible intelligence resources are requested for a specific purpose rather than collected for an over all purpose.[106]

Signal intelligence (Sigint)[107]

Signal intelligence can be divided into Communication Intelligence and Electronic Intelligence. Sigint does not often get much attention in the media although it often plays a crucial role in intelligence work. In the Cuban Missile crisis the crucial role of Photoint (Photographical Intelligence) and Humint has been publicized from the beginning through media.[108] The important part that Sigint played is little known to the general public. However, documents declassified and released in 1998, reveal the important part Sigint played in the Cuban crisis.[109]

---

[105] NSA recycles over 250 tons of paper a year. This figure indicates the enormous amount of public available sources that NSA collects every year. See " Facts and figures", online: http://www.nsa.gov:8080/about/, (date accessed: 17 July 1998)

[106] Intelligence can, dependent on the purpose of the intelligence and the source of the intelligence, be divided into several classes such as tactical and strategic intelligence. The term tactical refers to intelligence in a shorter time perspective and is intended to support for example brigade commanders with information support for military operations. Tactical intelligence are used by counterintelligence SOPs (Standard Operating Procedures) to provide operational intelligence. Strategic intelligence (also called National intelligence) has a broader object than tactical intelligence and is intended to serve firstly national security, secondly foreign policy and thirdly national economic purposes. Strategic interests include strategic military plans and doctrines, scientific and technical resources and development, NBC (Nuclear, Biologic and Chemical weapon programs.

[107] Modern Sigint dates back to the World War II. In the USA the use of Sigint disclosed Japanese plans to invade Midway during the war and it is believed Sigint shortened the war by a year. See "inside the NSA", online: http://www.nsa.giv:8080/docs/cuba/index.html, (date accessed: 17 July 1998)

[108] 'Photoint stands for photographic intelligence, which first and foremost are gathered with intelligence satellites.

Communication Intelligence (Comint)

Communication Intelligence refers to communication that carries information and encompasses signals carried by, for example, radio waves and wire. The information gathered may be coded and encrypted. Once the information has been decoded and decrypted it might also have to be translated from a foreign language.

Electronic Intelligence (Elint)

The branch devoted to electronic intelligence gathers intelligence from emitters that do not carry any readable information per se, such as radar. Analyses of the signal can nonetheless provide useful information. Radar emission tells the analyst the frequency used and can thereby help to identify the type of radar used.[110]

Human Intelligence

Humint is gathered through persons, either from open sources or clandestine. Persons such as for example military attaches, agents and special forces, collect human Intelligence.

---

[109] See "NSA and the Cuban Missile Crisis", online: http://www.nsa.gov:8080/docs/cuba/index.html, (date accessed: 22 July 1998)

[110] Elint (Electronic Intelligence) equipment is often located for example on ships in large spheres, in order not to reveal Elint capability. One example of Elint use was when US Sigint got indications of airborne radar fire control on MIG-17 and MIG-19 planes. See further "The Crisis Grows", online: http://www.nsa.gov:8080/docs/cuba/index.html (date accessed: 18 July 1998)

PART V International regulation of cryptography and the OECD Cryptography Policy Guidelines

5.1. International Regulation of Cryptography On the Internet

The purpose of this part is to describe and analyze the theoretical framework of the OECD Cryptography Policy Guidelines. The area of cryptography presents a new challenge for lawyers. We are standing in the face of a revolution, the cryptography revolution. Cryptography has many valuable uses but can, as most techniques, be abused. The possibility to, for example, use digital signatures and send documents or messages confidently is useful but cryptography may also, as described in part IV, have a negative impact on law enforcement and national intelligence capability. Should the use of strong encryption be regulated? If so, to what extent should it be regulated? A balance must be struck between, on one hand privacy/confidentiality and on the other hand, law enforcement/national security interests. The United States has earlier pushed for some kind or key escrow system or key recovery system. Sweden and other countries on the other hand have chosen to not prohibit export of strong encryption.

Since national interests are strong and contradictory in the area of cryptography it is important to reach an international consensus on which approach should be chosen. In this context the OECD initiative has to be welcomed. Which approach does the OECD agreement take and what legal questions will arise when the agreement is implemented internationally? No simple solution to the problem of concurrent law enforcement access and privacy exists. The solution is probably to balance the different interests, and as always when technological-judicial concerns are involved, to try and predict the future. We all know that this is not easy. However, a decision has to be taken after the different interests at stake have been balanced. What approach is the right one to take? My thesis is that we should let the market set a standard and avoid all forms of key escrow or key recovery systems since they will limit user trust, which is essential. I will elaborate on this viewpoint further below.

Introduction to International Regulation of Cryptography

While international electronic commerce continues to show rapid growth, one factor still holding back the real growth of e-commerce is the lack of security. Until the present problem with security has been solved electronic commerce will not be able to take off. The most promising techniques to enhance security in electronic commerce involve cryptography. Currently, many companies are developing encryption-based systems such as secure payment systems and digital money, which are essential for electronic commerce.[111] An area in which cryptography currently is used is EDI (Electronic Data Interchange). EDI exists both in closed networks and in open networks. Through EDI networks companies can exchange orders and other business information. Companies which are connected to EDI network presently use DES encryption to a large extent, but stronger encryption will be necessary to keep up with developments in computer and information technology, as well as developments in cryptoanalysis. The security problem is not of a technical nature, the difficulties lie rather in how to balance different domestic and international interests such as privacy, law enforcement and commerce.

The most promising technique so far to solve the problem with security in the Internet is public key encryption, which also offers security features such as digital signatures. However, the real benefits of public key encryption cannot be fully realized until an international agreement has been reached on international use of encryption and export of cryptographic products. Presently some countries such as Russia and Taiwan prohibit domestic use of strong encryption.[112] Other countries restrict the export of encryption products. Even though there is no monopoly on encryption products, the current U.S. dominance on software and especially Microsoft's dominance on operating systems limits compatibility.[113]Attempts to provide software that allows non-US encryption software to be added later have been thwarted as these interfaces have been

[111] For example CheckFree, Citicorp, CommerceNet, CyberCash, DigiCash, Electronic Payment Services(SmartCash), First Virtual Holdings, Mastercard, MCI Communications Corporations, Mondex, NetCash, Netmarket, NetScape, Open Market Security First Network Bank, ViaCrypt and VISA to mention a few. See further S. Godin, *Presenting Digital Cash,* 1 ed. (Indianapolis: Sams Net, 1995) at 240

[112] In 1997 use of strong encryption were limited or subject to a licensing scheme.

[113] Microsoft is supposed to have about 80 % of the world market on operating systems.

deemed to contravene United States regulations.[114] Security issues have to be dealt with on an international level, considering the border-less nature of data flows and international crime. No sender using the Internet can control which way the data is taking on the Internet. This means that encrypted files also are going to cross into countries which prohibit the use of strong encryption.

There are several difficulties that have to be overcome before an international consensus can be reached. One of these is the different views of privacy in e.g. the United States compared to EU member states.

A comparison of privacy legislation and case law shows the difference between the European view of privacy and the U.S. The American perspective is based on the Bill of Rights and focuses on the relation between the citizen and the Government and seeks to protect the citizen against Government intrusion. European countries on the other hand concentrate on the right to privacy in relation to business and the gathering of personal data for commercial use. It seems, however, that the American perception of privacy rights is moving closer to the European view. An example of this is the TRUSTe, which is an initiative championed by the CommerceNet and the Electronic Frontier Foundation. TRUSTe is an independent non-profit organization with two primary goals. Firstly, to accelerate growth of the Internet by promoting privacy disclosure and informed consent online. Secondly, to forestall prohibitive government regulation of online privacy.[115]

5.1.1 CoCom

The Coordinating Committee for Multilateral Export Controls (CoCom), dissolved in March 1994, was an international organization for the mutual control of the export of strategic products and technical data from country members to proscribed destinations. CoCom members agreed not to export militarily significant products with civilian purposes, especially to the East bloc, but also to what were considered as"rough"

---

[114] A. Marshall, "Encryption" (August 1997), issue 7 Internet Business Magazine, at 44.
[115] "ETRUST", online: Http://www.etrust.com/webpublishers/aboutus.html (date accessed: 10 October 1997)

nations.[116] Countries which had signed the agreement could more easily import and export products from other members.[117] One objective of the organization was to prevent cryptography from being exported to countries that supported terrorism. Countries to which export was restricted included Libya, Iran, Iraq and North Korea. Cocom maintained the International Industrial List and the International Munitions List. Pending the signing of a new treaty in 1994 most countries agreed to maintain the status quo and keep strong cryptography on their export control lists.[118] In 1991 CoCom had decided to allow export of mass-market cryptographic software. The United States, however, decided to retain separate regulations for cryptography. [119] There is reason to believe that cryptographic export restraints will not be much more successful than the CoCom regulations were.[120]

5.1.2 The Wassenaar Arrangement

In 1995 negotiations started on a new COCOM treaty. The negotiations were concluded in July 1996 and resulted in the Wassenaar Agreement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies.[121] The agreement was signed by a total of 31 countries.[122] The aim of the Wassenaar Arrangement is to control

---

[116] Crisis *Supra* note 67 at 231 and 435

[117] The original 17 member states were Australia, Belgium, Canada, Denmark, France, Germany, Greece, Italy, Japan, Luxembourg, The Netherlands, Norway, Portugal, Spain, Turkey, United Kingdom and the United States. Cooperating member states were; Austria, Finland, Hungary, Ireland, New Zealand, Poland, Singapore, Slovakia, South Korea, Sweden, Switzerland and Taiwan.

[118] "Wassenaar", online: http://www.wassenaar.org/docs/History.html (date accessed: 20 October 1999)

[119] "Bert Jan van Koops crypto pages", online: Http://www.cwis.kub.nl, (date accessed: 10 October 1997)

[120] William J. Perry, Deputy Secretary of Defense said during a breakfast meeting with Reporters, Friday, October 1993, on computer exports that "however much we want to control [computers] that are likely to be the retail mass market, it will be impractical to control them." He also noted the difficulties in trying to control export control in other countries:" "We have to recognize we don't have the ability to control computers which are available on the mass market from non-CoCom countries:" Mr Perry then noted the difficulties for the U.S. Government to set and control standards: "[the U.S. Government can no longer] "set the standards and specifications of computers. They are going to be set in the commercial industry, and our job is to try to adopt those if we want to stay current in the latest computer technology." (CRISIS at 310 note 3) The Crisis committee concluded that export of products with encryption capabilities are not qualitatively different. (*Crisis* at 310) The Crisis committee came to the conclusion that CoCom controls were less successful when; non CoCom members developed their own technologies, similar to those controlled by CoCom (which might be quite obvious), CoCom members did not agree with each other on risks with exporting certain products to Eastern bloc nations and finally the item in question was a dual-use item. All these factors are present in the current situation with cryptography.

[121] Dual-use means that the technology can be used for both commercial and military purposes.

[122] Argentina, Australia, Austria, Belgium, Canada, the Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Japan, Luxembourg, the Netherlands, New Zealand, Norway,

export of weapons and goods that can be used for military purposes. Cryptography is considered to fall under the classification of dual-use goods and it therefore falls under the Wassenaar Arrangement[123]. The arrangement is open to new members on a non-discriminatory basis provided they comply with certain criteria. A state must be a producer of industrial equipment or arms, maintain and adhere to proliferation regimes and treaties and have appropriate national policies, and finally maintain national export controls.[124] The member states commit themselves through national policies not to contribute or support development and enhancement of military capabilities that might undermine regional or international stability or security. Furthermore, participating states agree to maintain effective export controls for listed items, which are reviewed periodically as a consequence of technological advances and new possible uses. All changes to the list are made by consensus. Another facet of the agreement is the exchange of views and information.[125]

It is important to note that the Wassenaar Arrangement is not a treaty. Member states are thus free to implement the arrangement domestically and the members are free to determine the details of implementation. Countries to which export are restricted may therefore vary from member state to member state. The last review of the lists included a change concerning dual-use goods which was further extended to included hardware and software cryptography with more than 56 bits, or in some instances 64 bits in key length. The previous list of dual-use goods in the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual Use Goods contained a "General Software Note" that was difficult to interpret. [126] According to a press release the following amendments have been made: "The amendments to the lists included elimination of coverage of commonly available civil telecommunications equipment as

---

Poland, Portugal, the Republic of Korea, Romania, the Russian Federation, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, United Kingdom and the United States. Additional signatories are Bulgaria and Ukraine, which make the total number of founding members to 33.

[123] "Bert Jan van Koops Cryptopages", online:Http://www.cwis.kub.nl, (date accessed: 10 October 1997)

[124] *Supra* note 118

[125] *Ibid*

[126] Under the previous "General Software Note", the list did not control cryptographic software that was generally available to the public by being: a) Sold from stock at retail selling points without restriction, by means of:1. Over-the-counter transactions; 2. Mail order transactions; or 3. Telephone call transactions; and b) Designed for installation by the user without further substantial support by the supplier; or 2. "In the public domain". (The Wassenaar Arrangement as final approved in July 1996 Appendix 5)

well as the modernisation of encryption controls to keep pace with developing technology and electronic commerce, while also being mindful of security interests".[127] The new list is more comprehensive but contains also some exceptions e.g for. products accompanying their user, e.g. smart cards, portable or mobile radiotelephones not capable of end-to-end encryption. Moreover, there is a general provision, which excludes encryption products for the protection of intellectual property.[128]

5.1.3 Council of Europe

The Council of Europe is an intergovernmental organization, whose treaties are not applicable as law in the signing states. In a recommendation of 11 September 1995[129], the Council stated that " Measures should be considered to minimise the negative effects of the use of cryptography on the investigation of criminal offenses, without affecting its legitimate use more than is strictly necessary."[130] The statement shows that the Council of Europe favors some sort of restriction on strong encryption, but gives little further guidance.

5.2 The OECD and the Cryptography Policy Guidelines initiative

5.2.1 The OECD

The Organization for Economic Co-operation, based in Paris, is an intergovernmental organization set up to encourage co-operation in trade and investment amongst the governments of the Member countries. The OECD seeks to harmonize domestic policies in administrative and legislative matters. Directorates with experts from the Member states are established to form recommendations to Member states as well as non-member states. The global nature of world communications blurs national borders

---

[127] "PUBLIC STATEMENT" regarding the Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technology, Vienna, December 3, 1998, online; (http://www.wassenaar.org/docs/press_4.html (date accessed: 22 October 1999)

[128] "Dual-Use list- Category 5-Part II Information Security", online: (http://www.wassenaar.org/docs.html) (date accessed: 22 October 1999)

[129] R(95) 13 Concerning Problems of Criminal Procedure Law connected with Information Technology

[130] *Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology* (Adopted by the Committee of Ministers on 11 September 1995 at the 543 meeting of the Ministers' Deputies), online: http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.html (date accessed: 22 October 1999)

and forces countries to co-operate. The OECD offers a forum for its Members to discuss and study developments that restrict trade.

5.2.2 Earlier work done by the OECD to harmonize legislation regarding cryptography[131]

The OECD has previously dealt with security issues. Both the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data and the 1992 OECD Guidelines for the Security of Information Systems dealt with cryptographic technologies and social and economic issues related thereto. Security issues are therefore not a new challenge for the OECD. One of OECD's committees has since 1989 included studies of cryptographic technologies and methods in their work on security- and privacy issues.[132] The first OECD meeting that briefly touched upon cryptography questions was held in March 1990. Two expert meetings followed discussing cryptography technologies more thoroughly.[133] The latter of these meetings stressed that security, privacy and intellectual property protection issues must be balanced. None of these issues should dominate another or create unjustified obstacles to trade. [134] The first expert meeting concerning policy on cryptography was held on 18-19 December 1995 and gave the member states a possibility to discuss their policies. At the meeting the need for harmonized international cryptography policies and compatible national policies that strike the balance between data protection and law enforcement was stressed.

The private sector also played an important role in the development of the OECD Cryptography Policy Guidelines.[135] The first Business-Government Forum on Global Cryptography Policy was held on 19-20 December 1995. This meeting, which was held in conjunction with the ad hoc meeting, was organized by three parties; the

---

[131] "Report on Background and Issues of Cryptography Policy", online: http://www.oecd.org/dsti/iccp/legal/cryptpol.htm, (date accessed: 13 November 97)
[132] The OECD Information, Computer and Communications Policy Committee (ICCP)
[133] The Meeting of Experts on Recent Developments in Protection of Personal Data and Privacy held on 10-11 December 1992 and the Meeting of Experts on Information Infrastructures, held at the OECD 30 November - 2 December 1994
[134] It is worth to note that the same wording is used in principle 8 of the OECD Cryptography Policy Guidelines
[135] *Supra* note 131

OECD, the Business and Industry Advisory Committee to the OECD (BIAC) and the International Chamber of Commerce (ICC).

The United States proposal for the OECD to draft guidelines on cryptography policy was approved by the OECD Group of Experts on Security, Privacy and Intellectual Property Protection in the Global Information Infrastructure, in Canberra, Australia on 9 February 1996. The Ad hoc Group of Experts on Cryptography Policy was established shortly thereafter on 27 March 1996. The Ad hoc Group of Experts on Cryptography Policy began drafting the guidelines in May 1996. At the same time a second business-Government forum on global Cryptography Policy with representatives from the industry, Governments and advocacy groups was held. The guidelines were finished in record time. On a meeting the 27-28 January 1997, the Group of Experts on Security, Privacy and Intellectual Property Protection in the Global Information Infrastructure reviewed the draft guidelines. The OECD Council finally adopted the guidelines at its meeting on 27 March 1997.

Part VI The OECD Cryptography Policy Guidelines [136]

6.1 Background

The Guidelines are very broad in nature, which does not mean that the guidelines have not had any influence on national legislation regarding cryptography, information security- and privacy issues.[137] The Guidelines reflect the two major positions that existed when they were drafted: Member states advocating some kind of mandatory key-escrow, key recovery system or key management system and other countries advocating that the industry and the market should develop a standard.[138]

The United States, supported by Canada and Great Britain, were in 1997 the most dominant supporters of a mandatory system.[139] The Scandinavian countries, together with Japan, favored the market. As in all international negotiations compromises have to be made by all parties. The Guidelines show traces of these two views. Even though many countries already have enacted legislation regarding

---

[136] I will be using recommendation as a common term for the whole OECD Cryptography Policy Guidelines and not only the first part. Even though the recommendations are not binding for the member states the OECD Cryptography Policy Guidelines still are a carefully drafted international legal document, which I believe will have an impact on Member States cryptographic policies.

[137] It is of course not an easy task to negotiate international agreements and treaties on national issues such as national security and law enforcement, which are very closely connected to state sovereignty. Edward Cummings, legal adviser to the US State Department, noted in an panel discussion of the American Society of International Law (ASIL) that " a recent phenomenon of increasing importance – [namely] the negotiation of regimes that do not take the form of treaties". Remarks by Cummings, E.R. 89 *Proc. ASIL* (1995), at 380. Cummings further noted when discussing the characteristics of the Wassenaar Arrangement, that " [to] conclude a treaty could take forever, and it would probably never enter into force..." (at 382) He further concluded that "arms control – related agreements must generally be negotiated by consensus, and achieving consensus among 160 countries can take fifteen to twenty years. This is one reason why people are increasingly saying that we should negotiate agreements of a politically binding variety, because getting the real countries of concern to sign on to a treaty will take forever. (at 391) For a thorough examination of multilateral export control regimes see Ahlström, C, *The Status of Multilateral Export Control Regimes-An examination of Legal and Non-Legal Agreements in International Co-operation.* (Uppsala, Iustus, 1999)

[138] Different authors use the same terms for different meanings. The OECD guidelines themselves contribute to the present confusion by using key management as a euphemism for key recovery. In a key escrow system the keys are deposited with a third party. (The term trusted third party is not a good one to use because it brings one to think of key management systems), whereas the session keys are tagged along to the message in a key recovery system. The Government can, thereby get access to the keys when two parties are communicating before any transmission starts. In a key escrow system the chip key is already deposited.

[139] According to Prof. David Johnston, chairman of the IHAC (The Canadian Internet Highway Advisory Council) a report, which suggested that Canada should adopt a mandatory key system, was submitted in the fall 1997. See also "Bert-Jaap Koops Crypto Law Survey", online: http://cwis.kub.nl/~frw/people/koops/clc2.htm#co (date accessed 10 October 1998)

cryptography, the OECD Cryptography Guidelines serve as a valuable contribution to achieve international consensus.[140] Much criticism has been directed against the Guidelines as being too broad.[141] Earlier recommendations by the OECD, which also were heavily criticized when presented, has later become important for international legislation.[142] The Guidelines will therefore hopefully be one step towards harmonization of cryptographic policies around the world.

6.2 Earlier drafting on encryption and related issues

There are numerous examples of national and multinational legislation concerning encryption, security and related issues, such as privacy and intellectual property. However, very few attempts have been made to address encryption issues in an international perspective. This will be necessary to fully integrate an international information network. An integrated, global network is fundamental for international trade and electronic commerce.

The 1980 OECD Guidelines on the protection of Privacy and Transborder Flows of Personal Data and the 1992 OECD Guidelines for the Security of Information Systems mentions the importance of information system security for protection of privacy and personal data. Protection of personal data, privacy and confidentiality are very closely related to encryption. Legislation for protection of individuals with regard to processing of data and transborder data flows has been implemented in the European Union.[143] The Database directive requires the implementation of appropriate technical

---

[140] France and Russia restricted for example use of encryption in 1997 and the United States and Canada had enacted export controls that went further than the Wassenaar Agreement stipulated.

[141] When one looks back it seems that the OECD Cryptography Guidelines have had an impact on national cryptography policies. Canada's white paper on cryptography policy, *A Cryptography Policy Framework for Electronic Commerce building Canada's Information Economy and Society*, (Ottawa: Industry Canada) refers to the OECD Cryptography Guidelines: "The Government is committed to the development of a balanced policy framework, consistent with the OECD Guidelines for Cryptography Policy..." at page 12.

[142] I am especially thinking of the 1980 Guidelines on the Protection of Privacy and Transborder Data Flows of Personal Data and the 1992 OECD Guidelines for the Security of Information Systems

[143] *Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the protection of personal data and on the free movement of such data*, [1995] O.J.L .281/31 Available at:http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html

and organizational measures to protect personal data against accidental loss, alteration, or unauthorized disclosure or access.

The use of strong encryption has been subject to export controls for many years. The current basis for international export controls is the Wassenaar Arrangement mentioned earlier, which includes cryptography on the list of restricted export products. The underlying reason for export control in the Wassenaar Arrangement is to try to prevent export of munition to countries which do not respect fundamental democratic principles. The member states of the Wassenaar Arrangement have agreed to incorporate the Arrangement into national legislation. The United States' tough export controls have had a heavy impact on the international use of strong encryption since software companies in the United States control about 80 percent of the software market. To achieve a functional global use of encryption for electronic commerce encryption software needs to be compatible with the operating system. Electronic payment systems also needs to be user-friendly and seamlessly integrated in the operating system. The previous export controls in the United States severely restricted international use of strong encryption and software producers in the United States therefore criticized the Clinton administration for imposing unnecessary restrictions on the industry, thereby giving foreign software producers competitive advantages.

Article 17 Security of processing

1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.
Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.

2. The Member States shall provide that the controller must, where processing is carried out on his behalf, choose a processor providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures.

3. The carrying out of processing by way of a processor must be governed by a contract or legal act binding the processor to the controller and stipulating in particular that:
- the processor shall act only on instructions from the controller,
- the obligations set out in paragraph 1, as defined by the law of the Member State in which the processor is established, shall also be incumbent on the processor.

4. For the purposes of keeping proof, the parts of the contract or the legal act relating to data protection and the requirements relating to the measures referred to in paragraph 1 shall be in writing or in another equivalent form.

6.3 The Framework of the OECD Cryptography Policy Guidelines

The OECD Cryptography Policy Guidelines are divided into two parts. The first part describes and analyzes the legal context for cryptography on an international level. This part contains the recommendations to the member states. The second part contain the Guidelines themselves.

6.3.1 The Preamble to the Recommendations

The section starts, under the heading **having regard to,** with a list of policy documents, conventions, recommendations and directives the Council has considered and based the OECD Cryptography Policy Guidelines on. These international instruments formed a broad basis for what has been earlier negotiated and agreed upon. Most negotiating rounds are proceeded by several years of work and the final instruments are carefully framed. It would therefore have been detrimental to negotiate what has already been agreed upon again.

Under the heading **considering** the council states the underlying developments and reasons that form the basis of the recommendation. The Council emphasizes that we are living in a networked word with rapid development of national and international information infrastructure. This new global infrastructure will doubtlessly have an important impact on economic development and world trade. In this global infrastructure it is of fundamental importance that users have confidence in the security of information and communication infrastructures. This trust must embrace the confidentiality, integrity and availability of data. Ensuring data security through legal, procedural and technical means will be major tasks in order to achieve safe and trustworthy national and international telecommunication networks.
It should be noted that law enforcement issues and national security issues which play an important role in United States cryptography policy are not mentioned under **Considering,** but first under the heading **further recognizing**. The headline **Considering** must be interpreted as being more important than what is stated under the latter heading. The OECD Council therefore seems to have emphasized user trust more than national security and law enforcement concerns. In a study by JCP Computer

Services in 1997, they authors concluded that security was the chief concern of business and customers wishing to take advantage of electronic commerce.[144] The managing director of JCP, John Paleomylites has said: "The perception that the Internet is insecure is still the major obstacle to its widespread acceptance for electronic commerce".[145]

Security on the Internet is still today a major concern for users. Security is, however, no longer a technical problem. Technical solutions exist and cryptography is among the most promising new technologies. The difficulties lie rather on the procedural and legal level than the technical level. Once an international consensus has been reached the Internet offers massive cost savings. Electronic Commerce makes trading feasible for small companies and much easier for large companies since the entry barrier to new markets is lower on the Internet, making competition more effective. It will therefore be more difficult to uphold a monopoly or oligopoly. Marketing of new products is moreover easier and less costly on the Internet. A small company can potentially reach billions of customers from a website without a large advertising budget, which would have been necessary on the traditional market.

Under the heading **recognizing** the Council explains and states factors, which were taken into account when the recommendations and the guidelines were framed. This part can be divided into two further parts. The first part lists advantages with cryptography. The second part lists disadvantages and possible abuses of cryptography. This second part emphasizes one very important thing to keep in mind; use of cryptography to ensure integrity of data is distinct from use of cryptography to ensure confidentiality of data. These applications present different issues, but are also two sides of the same problem.

Under the second heading, **further recognizing,** the recommendation deals with more government related questions. This part aims at providing a counterpoint to the first part by stating that governments have many responsibilities and that cryptography can be used for illegal purposes. The guidelines seem to favor a market driven solution rather than a government driven solution. This is indicated by the use of "may" under the second paragraph and by the fact that the enforcement of laws and national security is listed last under the first paragraph. The last two bullets in this section contradict in

---

[144] G. Leeming, *A New Business Paradigm* , (August 1997), issue 7, Internet Business Magazine, at 37
[145] *Ibid* at 36

my opinion each other. The Council first emphasizes that the Internet is global in its nature and that the removal of incompatible national policies will have to be made to meet the needs of businesses, individuals and governments. On the other hand the nature of the recommendation as non-binding on the member states is emphasized in the next section. The recommendation stresses the need to remove obstacles and then in the same breath adds that states are sovereign and therefore may deviate from the recommendations.

6.3.2 The Recommendations

On the proposal of the Committee for information, Computer and Communications Policy;

RECOMMENDS THAT MEMBER COUNTRIES:

1.establish new, or amend existing, policies, methods, measures, practices and procedures to reflect and take into account the Principles concerning cryptography policy set forth in the Guidelines contained in the Annex to this Recommendation (hereinafter "the Guidelines"), which is an integral part hereof; in so doing, also take into account the Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data of 23 September 1980 [C(80)58(Final)] and the Recommendation of the Council concerning Guidelines for the Security of Information Systems of 26-27 November 1992 [C(92)188/FINAL];

Regulation of cryptography is diverse in the OECD member states and the recommendation underlines the importance of harmonizing national legislation by adherence to the principles set out in the guidelines. The Guidelines shall in that respect serve as a yardstick.

2.consult, co-ordinate and co-operate at the national and international level in the implementation of the Guidelines;

This recommendation is further outlined together with the third and fourth recommendation in the Guidelines under principle 8 which calls on governments to co-operate on and co-ordinate cryptography policies. As part of the effort to co-ordinate and co-operate governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade. Co-ordination on the national level has to be left to member states. One can hope that states at least are coordinating their own national regulations. The recommendation states "**national and international** level", which suggests that the council wants to see a transborder harmonization between governmental agencies. It is to me not clear what the Council means in this respect. Co-ordination is currently, except for within the OECD, taking place in several

forums such as in the European Council and in the International Chamber of Commerce in Paris.

3.act on the need for practical and operational solutions in the area of international cryptography policy by using the Guidelines as a basis for agreements on specific issues related to international cryptography policy;

This recommendation calls for more compatible, interpretable, portable and mobile cryptographic methods. It reflects what is more broadly covered in the Guidelines under principles 2, 3 and 4. These three guideline principles reflect the choice of cryptographic methods and standards throughout market driven development.

4.disseminate the Guidelines throughout the public and private sectors to promote awareness of the issues and policies related to cryptography;

The principle emphasizes the need for an open public debate where the Guidelines can be useful as a starting point. The conditions for lawful access are further explained in principle number 6. In this principle the importance of transparency of conditions for lawful access is emphasized.

5.remove, or avoid creating in the name of cryptography policy, unjustified obstacles to international trade and the development of information and communications networks;

Export of strategic products to certain countries has been restricted through the Wassenaar Arrangement on the basis of their close relationship with terrorist organizations. Some countries such as the United States have enacted yet more restrictive export policies. This recommendation shows how vague the guidelines are. The word unjustified refers to law enforcement and national security reasons. Part II of the Guidelines, **Scope** clarifies the exception by stating;" It is recognized that governments have separable and distinct responsibilities for the protection of information which requires security in the national interest; the Guidelines are not intended for application in these matters." Interpretation of "unjustified" and the concept of national interest embraces most national policies. The Guidelines have been criticized for being too vague and too flexible and they are indeed vague in this recommendation. The recommendation first condemns obstacles to international trade, which the United States export controls must be considered as, and then opens up a possibility to exclude the whole area by a broad exception. Although the Guidelines

indicate a more privacy-oriented policy it is clear that states are free to chose between a privacy-oriented or law-enforcement oriented policy. One wonders if states will be able to reach consensus which is absolutely necessary. The race, supported by supporters of both camps, towards an international standard has started. Even if Member states have accomplished much, a long way still remains to go to achieve international consensus.

6.state clearly and make publicly available, any national controls imposed by governments relating to the use of cryptography;

This recommendation examines cryptographic policy and pulls national policies out of the shadows where they have been hidden many years. Cryptographic applications are presently more focused on civilian than military use, even though the military stood behind much of the development of cryptographic applications.

7.review the Guidelines at least every five years, with a view to improving international co-operation on issues relating to cryptography policy.

The suggested review of the guidelines every five years is not appropriate. If it should have any effect, review should be made with shorter intervals considering the rapid development in these areas. A review of the Guidelines, for example every second year would spur changes in national policies.

Analysis of the Recommendations

Several of the recommendations do not give much guidance alone but rather refer to the guidelines, which are much more detailed. The recommendations can, in several cases, be seen as an introduction to the guidelines. It therefore seems that the guidelines should be assigned almost the same weight as the recommendations.

6.4 The Guidelines

The Guidelines attempt to negotiate interests which seem incompatible. It is my belief that it is not possible to balance privacy and security interests on the one hand and law enforcement access and national security interests on the other hand in a single national cryptography policy. In the end a choice has to be made. After the choice has been made a careful analysis has to take place to analyze eventual discrepancies that exist and the measures that can be taken to restore a sound balance. The Guideline part of the OECD Cryptography Policy Guidelines are divided into 5 headings: I Aims, II Scope, III Definitions, Integration and V Principles. Section IV of the Guidelines states that each of the principles in section V are interdependent and should be implemented as a whole to balance the various interests at stake. Moreover, the section states that no principle should be implemented in isolation from the others.

When implementing the principles a broad view has to be taken and the situation has to be evaluated after the choice has been made. The uncertainty that presently exists is far more detrimental to international business than accepting some kind of a mandatory key access system. One might wonder what political considerations underlie the U.S. Government attempts to establish a mandatory key access system. However, the real reason might be that there is no considered careful policy and no action plan behind the present national cryptography policy. The argument that access to strong encryption would hinder law enforcement has not been very convincing. The real reason for keeping the status quo as long as possible is in order not to lose intelligence capacity.

Aims

The aims are very closely related to the recommendations themselves and in fact, to a great extent, repeat to some extent what has already been dealt with in the recommendations. As a first and foremost aim the Guidelines are said to promote the use of cryptography. The promotion has two goals; to foster confidence in information and communication infrastructures and to foster confidence in the manner in which the Guidelines are used. The Council is here aiming at information and communication networks.[146] Another goal for promotion of cryptography is to ensure the security of

[146] How cryptography will help foster confidence in the manner the systems are used is hard to understand.

data and privacy. According to these goals promotion of cryptography has to be done without unduly jeopardizing public safety, law enforcement and national security. These aims seem to be a compromise forced by countries favoring mandatory key access systems. The aims demonstrate the vagueness of the Guidelines. From my point of view it would have been more favorable approaching it from an international perspective and promoting that objective rather than trying to promote two incoherent and incomprehensible aims and then leaving it up to the member states. After all, the recommendations and the Guidelines incorporated therein are in any case non- binding.

Scope

I have criticized above the exception concerning matters of national interest as being to broad. These irreconcilable objectives are stated again in the part Scope. The Council emphasizes, moreover, under the heading scope in the recommendations that the Guidelines should be widely read and followed by, not only Government, but also private and public sectors. This brings us to the principles themselves.

The Principles

The part with the actual Guidelines consist of seven principles intended to give national governments guidance when formulating and developing national policies. The principles are more clearly and forcefully drafted than the recommendations. They also cover some areas that are mentioned in the recommendations. Alongside the principles, explanatory notes are added to further explain and clarify the principles.[147] The principles should, however, be given preference in relation to the explanatory notes when interpreting the Guidelines.

6.4.1 TRUST IN CRYPTOGRAPHIC METHODS

CRYPTOGRAPHIC METHODS SHOULD BE TRUSTWORTHY IN ORDER TO GENERATE CONFIDENCE IN THE USE OF INFORMATION AND COMMUNICATIONS SYSTEMS.

Market forces should serve to build trust in reliable systems, and government regulation, licensing, and use of cryptographic methods may also encourage user trust. Evaluation of cryptographic methods, especially against market-accepted criteria, could also generate user trust.

[147] The explanatory notes are shown in italics in this thesis. The principles are shown in upper letter cases.

In the interests of user trust, a contract dealing with the use of a key management system should indicate the jurisdiction whose laws apply to that system.

To establish user trust is a fundamental goal for any national cryptographic policy. Several surveys show that privacy and security concern is what worries users most.[148] In particular, for electronic commerce to take off it is essential to establish a solid trust.The principle of trust is rather straightforward, but the explanatory text below is harder to interpret. It is not surprising that the drafters of the OECD Cryptography Guidelines have put the principle of trust first because it has a bearing on all the other principles in the Cryptography Guidelines. A free choice of cryptographic methods, reliable standards and a thorough protection for personal privacy and personal data will presumably result in greater trust in cryptographic methods. Most important for user trust in cryptography is a transparent and consistent regulation of lawful access and liability. Failure in implementing these principles adequately will result in less trust and thereby less use of cryptographic methods.[149] Harmonization of divergent cryptographic policies is, moreover, needed because of the global flow of data. Such and harmonization can only be achieved through greater international co-operation.[150]Full confidence in cryptographic methods will never be achieved, but user confidence has to grow much stronger than it is today.

Government regulation-A legal and contractual framework

---

[148] In a survey by Navidec in July 1999, 36 percent expressed concern about the security of shopping online. Of these only 21 percent were worried for credit card fraud. ("Navidec Inc: 53 Percent of US Users Have Bought Online" (15 July 1999), online http://www.nua.ie/surveys/index.cgi?f=VS&art_id905355027&rel=true (date accessed: 22 July 1999)

[149] Reports of trap doors and backdoors into a variety of different computer programs are detrimental for user trust in cryptographic methods. According to a report issued by the European Parliament's Science and Technology Options Panel (STOA) something called a "workfactor reaction shield" was built into Lotus Notes and incorporated into all a-mail sent by non-US users. The trapdoor was first reported by a Swedish newspaper, Svenska Dagbladet in 1997 to the embarrassment of Lotus. Issues like this of course makes users hesitate as to which programs they can trust. The report can be accessed online. "Development of surveillance technology and risk of abuse of economic information", http://www.gn.apc.org/duncan/stoa_cover.htm, (date accessed: 5 December 1999) See also Wired *Spying on the Spies,* (10 May 1999), online: http://www.lycos.com/print/0,1294,19602,00.html (date accessed: 5 December 1999)

[150] Currently the Scandinavian countries has a more liberal view to cryptography than for example the United States of America, which is the greatest advocate for export control and international regulation of encryption. The Scandinavian countries are, moreover, more focused on privacy protection than the U.S.A. and Canada.

The electronic environment is, in conformity with the current world, not without risks when for example consumers are making purchases. The risks for the consumer in the traditional legal environment of today are, however, well defined or at least predictable. On the other hand there is a considerable uncertainty regarding electronic transactions over the Internet. It is primarily when the value and advantages of electronic commerce are greater than the risks that consumers will embrace electronic commerce fully.[151] It is therefore important that a legal framework is put into place which enables the consumer to assess the risks. In order to make the legal framework effective it has to be complemented by contracts regulating these issues in the private sector. If the consumer is using his credit card when paying for goods over the Internet it is still unclear in some jurisdictions to what extent the cardholder might be held liable. For the consumer it is of course important to know how much money he risks losing if somebody, for example, intercepts his credit card number and uses it.

For electronic commerce to take off it is essential that allocation of risks between buyers, sellers and third parties, such as financial institutions, is clarified. Probably a great deal of the existing framework, for example of credit card transactions, can be applied. Analogies can also been drawn from international conventions such as the Warsaw convention regarding difficult issues such as liability.[152] Electronic commerce is going to make international transactions increasingly common and an international regulatory network is needed to establish user trust.[153] In particular the liability issue will be difficult to solve, especially in an international context.[154]

---

[151] See "Report on Background and Issues of Cryptography Policy", online: http://www.oecd.org/dsti/iccp/legal/cryptopol.htm, (date accessed: 13 November 1997)

[152] The Convention for the Unification of Certain Rules Relating to International Carriage by Air signed at Warsaw 12 October 1929. Amended at the Hague, 28th September 1955 For further information see "Draft convention for the modernization of the Warsaw system of air carrier liability approved" available online at http://www.icao.org/icao/en/nr/pio9709.htm

[153] Litigation issues can be difficult to solve since there is no international small claims court. The only international court is the (ICC) International Chamber of Commerce based in Paris. Considering the cost of international litigation the ICC is not a realistic alternative. Consumer protection legislation in several countries also prohibits prorogation clauses in consumer contracts. From a law and economics standpoint costs for losses attributed to electronic commerce should preferably be carried by financial institutions. Financial institutions can later on transfer the costs to business and consumers. If the cost for losses are attributed to financial institutions then the financial institutions will have an incitement to minimize loses and continuously improve the security of the framework. It would, moreover, be more cost effective if the cost for improvement was carried by financial institutions, e.g. credit card companies and then transferred to the customer. It is, however, reasonable that user carries the cost for losses he has not exercised due diligence If e.g. a user has not been acting with due care and as a "reasonable man" he should carry the

Market Forces

The explanatory principle mentions "market force," but what is the market force? No definition is given in the Cryptography Guidelines of this term. It can, however, be presumed that "the market forces" under this principle are a combination of users and producers of cryptographic systems. Users should include individuals, businesses and governments. Producers should include businesses and governments.[155] Reading between the lines the Cryptography guidelines are making the point that trust has to be built; it cannot be imposed. The Clinton administration's flawed attempt to introduce a de facto standard by public procurement power was seen by the American public as a government intrusion to privacy and therefore the attempt fell flat.[156] Standards are also based on user trust in one or another way and do not become de facto standards until they are fully embraced by the users.

Reliable systems

A wide range of cryptographic products exist today. Many of these products are however of doubtful quality.[157] Generally, governments have the best resources to evaluate cryptographic systems and methods. It would therefore be preferable if governments could take a leading role in establishing reliable criteria for evaluating

---

cost for the loss. A balance has to be achieved so that the one who can control the risk and has the financial capacity to improve the surrounding system should bear the risk.

[154] I will return to the issue under the liability principle in Part V.

[155] This definition of market forces can be concluded by the principle of free choice in which "market forces" is mentioned in the title. In the principle itself individuals, business and governments are mentioned. Strangely, there is no reference to the title however.

[156] The attempt by the Clinton administration has been criticized from several points of view. Some critics have alleged that it was a circumvention of congressional powers, others that it was an attempt by the NSA to dictate domestic cryptography policy. Looking back, one can establish that the attempt did more harm than good to the administrations' intentions.

[157] For evaluation criteria of cryptographic systems see Applied Cryptography, *supra* note 46 at 214

cryptographic methods.[158] Cryptographic algorithms should also be open to public scrutiny.[159]

Licensing and governmental use

Governmental licensing will in particular be important for Certification Agencies(CA).[160] A major problem with public key infrastructures is key management. The link between the key holder and the public key has to be verifiable. This can be done by a certification authority. Exactly what the licensing framework will look like is not clear. Different models will probably surface. One structure would be to have a national top CA that licenses a few national CAs. A legal framework for the conditions under which CAs operate has, moreover, to be established. Presumably most major corporations would wish to have a corporation CA. It is important that governments take an active role in the use of cryptography establishing CAs and furthermore that they actively support the establishment of neutral open standards. Preferably, governments should take a supporting, instead of a leading role in the development of cryptographic standards.[161]

Applicable jurisdiction and key management systems

The last paragraph in the explanatory text "In the interest of user trust..." (See above) is incorrectly placed according to Stewart Baker.[162] At first sight it seems indeed odd that

---

[158] This presupposes of course that governments are trusted and can act objectively, which might not always be the case. A problem is where the competence in evaluation of cryptographic systems is gathered. In for example the USA, the NSA probably has the best competence to evaluate and scrutinize cryptographic methods. Many organizations would however probably object to the NSA evaluating products since they would question their objectivity.

[159] If cryptographic algorithms are secret there is of course an additional step to break the cryptographic system if the algorithm is secret. From the user perspective and from the perspective of user trust it is however essential that the algorithms used are scrutinized publicly.

[160] Another name for CA (Certification Authority) is Trusted Third Party. The later term is more used in Europe.

[161] Dependent of course if the government can be trusted as objective. The failed attempt by the US Government to impose Federal Processing Standards (FIPS) though government procurement power did not exactly increase the creditability of the Clinton government in the eyes of privacy organizations.

[162] "Decoding the OECD's Guidelines for Cryptography Policy", online: http://www.steptoe.com/comment.htm, (date accessed: 2 November 1998) at 7. [hereinafter *Decoding*] Stewart Baker is a former general counsel to the NSA and participated in the Ad Hoc Group of Experts on Cryptography Policy Guidelines (Ad Hoc Group) that drafted the Guidelines. The first discussion draft was, however, drafted by the United States Council for International Business (USCIB) See *Decoding ibid* at 4

such specific explanatory text has been put in with the trust principle. The Report on Background and Issues of Cryptography Policy does not clarify very much either: "In that context, it is also important for users to understand the legal framework which governs their use of cryptography, particularly in light of the "borderless" nature of information and communication networks".[163]

Baker is of the opinion that the sentence either is what it prima facie looks like- a choice of law clause- or else related to lawful access of keys.[164] As a choice of law clause it might have some bearing on consumer trust. Baker concludes, however, that such a reading is unlikely because the text is too detailed and tenuously tied to the trust principle to belong in the explanatory text to this principle. The other possible reading offered by Baker is that the sentence relates to contracts dealing with management of keys and lawful access to these keys

> "Arguably, the sentence requires that contracts for the management of keys list all of the nations that have jurisdiction to demand lawful access to the keys. If so, it is a potentially sweeping rule aimed squarely at the private sector, and as such, a deviation from OECD's traditional approach of making recommendations to governments. Even if it read simply as encouraging governments to adopt this rule in setting for the private sector, it is also likely to prove unworkable. In many cases, determining which jurisdictions might be able to order production of cryptographic keys is a complex legal task.... The prospect of such a burden will naturally lead companies to ask whether this statement actually imposes any obligation on them. An OECD document cannot create obligations on its own; particularly is this so with respect to stray statements in explanatory text rather than recommendations or principles. Even if the statement could be read as imposing an obligation on private actors, it applies to a limited ill-defined class—persons or entities that have contracts dealing with the use of a key management system"[165]

Baker concludes that the phrase "contract dealing with the use of a key management system" should be interpreted to mean that it only applies to companies that explicitly and exclusively act as "key recovery" agents, i.e. companies who solely deal with key

---

[163] Report on Background on Cryptography *supra* note 131 at 4 .
[164] Decoding *supra* note 162 at 8
[165] This interpretation is supported by Steve Orlowski, "Cryptography Policy--OECD Cryptography Guidelines"(1997) 13:4 Computer Law & Security Report, Elsevier Science at 275 [hereinafter Orlowski]. Steve Orlowski is a Report Correspondent Special Adviser for IT Security Policy in the Information and Security Law Division at the Australian Attorney General's Department

management for lawful access. The explanatory text, moreover, alludes to the fact that users need to know where keys are held:

> "The text supporting this principle also makes the point that users who use key management systems need to know in which country their keys will be held, and consequently what lawful access legislation may apply to those keys. Without such knowledge user may not trust cryptographic methods which incorporate key management systems."[166]

The keys might, however, be held in several countries. The presumption that the law of the jurisdiction which the keys are held governs conditions for lawful access to the keys does not have to be true. What is most important to know for the user is who is liable for the keys and who has access to the keys. The explanatory text is unclear on this issue.

A source of confusion in the Cryptography Guidelines is the broad definition of "key management system" as a system for "generation, storage, distribution, revocation, deletion, archiving, certification or application of cryptographic keys." There is no term in the guidelines reserved for law enforcement access to keys, albeit governmental access and user access rest on different grounds.[167]

An analysis of trust from an economic point of view

---

[166] *Ibid* at 276

[167] When the Clipper Chip was introduced the term key escrow was the general term. Two custodians kept the keys in escrow. As a result of the fierce debate the term key escrow become tainted and fell out of use. Another term was then introduced, key recovery. This term meant that the keys were not held in escrow in advance, but they had to be accessible. The term key management systems have traditionally been used as a more general term for handling of keys. All countries with a public key infrastructure will have to have some form of key management system, but not necessarily a key escrow or key access or key recovery system designated to give law enforcement agencies access to keys. There is a need to differentiate between the terms. Terms used in the Cryptography Policy Guidelines should refer to the general meaning or define the intended meaning otherwise the term will be misleading. The term "Law enforcement" in the Cryptography Policy Guidelines is put on an equal footing with enforcement of laws. In my opinion enforcement of laws is broader and much more general than law enforcement, which usually is used with reference to police work. Another term introduced by the Cryptography Guidelines is lawful access. Lawful access is defined in the Guidelines as "access by third party individuals or entities, including governments, to plaintext, or cryptographic keys, of encrypted data, in accordance with law". In my view the guidelines should make a distinction between public access by law enforcement agencies or national security agencies, and other kind of access from, for example users or employers. Access by law enforcement and national security agencies has to be governed by law. This is not the case with access for employers and users. In this case it can be dealt with by contracts. The reasons why a distinction should be upheld is that they touch upon two different areas of law, public and private. It is, however, hard to see any reason for not separating them.

A fundamental prerequisite for a market economy is a judicial system, but why is a judicial system necessary? In a society with no legal order a situation called the prisoners' dilemma is supposed to exist. The prisoners' dilemma represents a basic stage in economical development.[168] In the prisoners' dilemma both parties gain by trading and cooperating with each other.[169] By trading people can specialize and become more efficient, moreover people can get access to goods and services they cannot get or perform themselves. Both parties can, however, gain more by robbing and defrauding each other. What is then holding them back? If both parties trust each other and picture long term gains by continuing to trade with each other none of the parties will disrupt the trust and endanger business in a longer perspective.[170] A complex market economy requires a judicial order. It is, however, also necessary that the judicial system is trusted. Trust in the judicial system may partly substitute for trust in whom you are trading with. A party can enforce a contract against a non-performing counterparty that is not fulfilling the contract with the help of the judicial system(pacta sunt servanda).[171] Both systems are thus dependent on each other.

It should be remembered that fraud, theft, forfeiture, etc, will continue to be present in a digitized world. Fraud has especially been a thorn in the side to finance

---

[168] The prisoners' dilemma was originally formulated by the mathematician Albert W. Tucker. Two robbery suspects are isolated separately and are urged to confess. Each of them must decide whether to confess or remain mute without knowing the other one's decision. If both confess, both go to jail for five years; if neither confesses, both go to jail for one year; and if one confesses while the other does not, the confessor goes free and the silent one goes to jail for 20 years. If they both act selfishly and confess hoping that the other one will remain mute, they face up to twenty years of prison. If they, instead, remain silent and thereby unselfishly cooperate, each would only serve only one year in prison. The dilemma is, that they do worse when they do not cooperate than when they act unselfishly. See also Göran Skogh ed., *Den osynlige handen och lagens långa arm,* in Ekonomi under Debatt, Göran skogh ed (Malmö, Liber, 1983) [hereinafter *Skogh*] at 11.

[169] The theory that one might gain more by cooperation and trust is not new. Thomas Hobbes described in the *Leviathan, (1651)* Part I and II (Indianapolis: Bobbs-Merril, 1951) how people, in order to avoid an all-out-war, conclude a social contract with each other. Also Rousseau assumed that citizens were willing to accept a constitutional order to gain advantages. (J-J Rousseau, *The Social Contract, (1762)* (Harmondworths: Penguin Books, 1968)

[170] See also about economic theory: D.Luce & H. Raiffa, *Games and decisions,* (New York, John Wiley & Sons, 1957) and A. Schotter, *The Economic Theory of Social Institutions* (Cambridge: Cambridge University Press, 1981)

[171] An example hereof is the present situation in Russia where a breakdown of the judicial system and financial system is starting to take place. In general when a judicial system breaks down, or the trust in the judicial system diminishes, people rescind to a more primitive stage of economic development. People start to trade goods and services directly with each other instead of doing what they are good at. Doctors cultivate beets instead of working in their profession, which would be more beneficial for both the doctors and the society. Through the gradual breakdown of the judicial system in Russia a fundamental pylon of the market economy has diminished.

houses and credit companies. The Internet enhances the opportunity for fraud since it is more anonymous.[172] Fraud can also be committed in a wider scale in an international arena. The international aspect creates difficulties with different jurisdictions and conflict of laws on the Internet. Protection against malicious behavior lies, as is mentioned in the preamble to the recommendations, in good managerial, organizational and operational procedures. International use of cryptography will probably reduce the possibilities for criminal conduct. Security in information systems will, however always be dependent on their users. If people write down their private or secret keys the risk of fraud committed by somebody who gets hold of these keys is probably greater than before because people tend to blindly rely on technical systems.[173]

Technical systems always function within given parameters. This is also the case with cryptography. It is here that management systems come into play with possibilities for revocation of keys that have been compromised. It is the user who should control the technology, not the opposite. A substantial number of legal issues regarding management of keys need to be dealt with to make the system work. Electronic Commerce on the Internet will require a much closer integration of national laws than ever before, especially regarding liability issues and conflicts of law. The challenge is threefold: developing and implementing the technology, planning for avoiding the failures of the technology; and gaining public support for and approval of the use of the technology.[174]

Ongoing developments

[172] The major credit card companies lose more than 1 billion dollars a year in credit card fraud. See Per Odebrant "Bankerna förlorar 63 kr i sekunden, (1999) no 4, Aktuell Säkerhet at 24

[173] In a flight simulation test by a US team of researchers at the University of Illinois 40 percent of the pilots in the test trusted the computers and did not take action, compared to 3 percent in the reference group. The Korean plane that was downed by Russian fighter plans is believed to have deviated from the course because the autopilot was on and the pilot failed to check that the autopilot computer gave reliable course indications. See Ulrika Björkstén, "Autopilot invaggar pilot i falsk säkerhet", 1999, Svenska Dagbladet 5 December at 11.

[174] Report on background and issues of cryptography policy *supra* note 151

In November 1999 the European Commission presented a new European Directive on Electronic Signatures, which marked another step towards greater harmonization.[175]

6.4.2 CHOICE OF CRYPTOGRAPHIC METHODS

USERS SHOULD HAVE A RIGHT TO CHOOSE ANY CRYPTOGRAPHIC METHOD, SUBJECT TO APPLICABLE LAW.

Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communications systems, and the confidentiality and integrity of data on those systems. Individuals or entities who own, control, access, use or store data may have a responsibility to protect the confidentiality and integrity of such data, and may therefore be responsible for using appropriate cryptographic methods. It is expected that a variety of cryptographic methods may be needed to fulfill different data security requirements. Users of cryptography should be free, subject to applicable law, to determine the type and level of data security needed, and to select and implement appropriate cryptographic methods, including a key management system that suits their needs.

In order to protect an identified public interest, such as the protection of personal data or electronic commerce, governments may implement policies requiring cryptographic methods to achieve a sufficient level of protection.

Government controls on cryptographic methods should be no more than are essential to the discharge of government responsibilities and should respect user choice to the greatest extent possible. This principle should not be interpreted as implying that governments should initiate legislation which limits user choice.

The principle of free choice is the basis for the principle of trust.[176] The emphasis on the user runs coherently throughout the guidelines. Exceptions from the main principles are stated, not only in the sentence entitled the "scope", but also sometimes in the principles themselves. This principle reflects the two different views that exist: free use of strong cryptography, as opposed to restrictions in use, import and export. In this principle the free choice principle has been made subject to applicable law so as to emphasize that the free choice may be restricted.

Subject to Applicable Law

"[A]pplicable law" refers to national law which might impose for example a certain minimum key length or limit use of choice to certain cryptographic methods.[177] This exception from the main principle is an example of how the different underlying views on cryptography have affected the Guidelines. Some OECD countries like France have

---

[175] Council Directive 1999/93 of 13 December 1999 on a Community framework for electronic signatures [2000] O.J.L 13/12

[176] See the explanatory text under the principle of free choice in Part VI.

[177] See the Cryptography Guidelines under the title "AND FURTHER RECOGNISING", which states; "that this Recommendation of the Council does not affect the sovereign rights of national governments

imposed far reaching restrictions on the domestic use of cryptography.[178] Other OECD countries, for example the USA, have more restrictive export controls than most other countries in the world.[179] The USA has tried to persuade other OECD countries to implement a mandatory key access system. In a mandatory key-access-system user choice must by necessity be limited, either by technological means or by legislation. In e.g. the Clipper chip communication between the two parties is restricted by the way the chip operates. Communication is only possible if exchange of LEAFs (Law Access Exchange Fields) has taken place prior to the private conversation or communication.[180] In a software key escrow system like the one presented by the United States Government in 1997, communication through unauthorized protocols is barred by the software.[181] The software will only function with other allowed systems that have a backdoor to the algorithm used for encryption. Any country adopting a mandatory key management system must by necessity restrict the number of allowed cryptographic systems or else systems for the revocation of keys will in turn become too complex.

---

and that the Guidelines contained in the Annex to this Recommendation are always subject to the requirements of national law:"

[178] France introduced a new policy in the beginning of 1999 when Prime minister Lionel Jospin announced that France's complex licensing schemes for import and domestic use and mandatory key registration requirements would be abolished. According to the statement France will permit the use of strong encryption domestically in France. France will, however, maintain its export controls in accordance with its international engagements. See "Discours et Interventions", online: http://.premier-ministre.gouv.fr/PM/D1901999.htm, (date accessed: 24 October 1999) Also the USA has announced a new approach to encryption according to a press release from the White House Office of the Press Secretary September 16, 1999. According to the press release any encryption commodity or software of any key length can be exported under a new license exception, after a technical review, to commercial firms as well as non-government end users, except to seven countries that the USA considers to be supporters of terrorism. (White House Fact Sheet; Administration Updates Encryption Export Policy, Law and the New Policy, online: http://www.steptoe.com/webdoc.nsf/83/doc6dc16e7abd3852659f00499doq/10cfb7b70e573152852567f3005a07b5?Open Document, (The White House, Office of the Press secretary, September 16, 1999) (date accessed: 16 November 1999.)

[179] In France one previously needed a license to use strong cryptography. Also the Netherlands tried to introduce restrictions on the use of cryptography. The proposal in the Netherlands met, however, strong opposition. It must be underlined that most of the OECD countries have signed the Wassenaar Arrangement and therefore has exports controls. Some countries such as the USA and Canada have, however, chosen to restrict exports more than the Wassenaar arrangement stipulates.

[180] A. M. Froomkin, "The Metaphor Is The Key: Cryptography, The Clipper Chip And The Constitution", (1995), 143, University of Pennsylvania Law Review 709, at 753

[181] The Clinton administration has since 1993 considered escrowed encryption as a basic pillar of their national cryptography policy and aggressively tried to promote it nationally as well as internationally. Public concern has however focused on the possibility of failure in the system that will allow access to the cryptographic keys and loss of confidentiality. See Crisis *Supra* note *67* at 112.

In the aims of the Cryptography Policy Guidelines it is stated that the guidelines are intended to promote the use of cryptography, help to ensure the security of data and to protect privacy. Use of cryptography should, however, according to the explanatory text, be made without unduly jeopardizing public safety, law enforcement and national security. How this balance should be struck is not explained anywhere in the guidelines, but is left to the Member States. In the explanatory text it is stated that governmental control over cryptographic methods should not be more than is essential. What does this mean? In my view it means that restrictions on cryptographic systems have to be justifiable by reference to a concrete aim of national policy that outweighs the resultant limitations on free choice. Reasons for restrictions to limit free choice should, moreover, be made public; a mere vague reference to national security is not enough. It is important that the choice is left to the user because the user will chose a cryptographic product that corresponds to his needs and budget. It is most efficient both for the individual and the industry. By leaving the choice to the user the cost of implementing the system will be less than if restrictions are imposed.

The cost of developing cryptographic systems and maintaining them will furthermore be borne by the private sector. In a system with government key access like the Clipper chip the Government will have to absorb a larger portion of the cost. Strict law and economic arguments can therefore be raised for leaving the development of cryptographic systems to the market. When a user chooses a particular cryptographic system he has to take into consideration the value of the information, potential threats to his communication and information that exist, the number of encrypted messages he is going to send and the length of these messages; Furthermore, he will have to take into consideration how quickly he needs the messages or data to be encrypted. These latter two factors will depend on the user's computing power and the intrinsic features of the chosen encryption system. Usually a hardware system that is designed only to encrypt works more efficiently and faster than a software based encryption system. It is however not always necessary for the user to encrypt the whole message since private messages often are rather less sensitive.

The ordinary user is likely therefore to be more concerned with authentication than confidentiality. It can be assumed that users who are not doing business and need strong encryption, will use systems that are less complicated. They will focus on the

price of the product in relation to what they need. What most users probably are looking for is also cryptographic systems that can be seamlessly integrated with their other software, such as browsers.

6.4.3 MARKET DRIVEN DEVELOPMENT OF CRYPTOGRAPHIC METHODS

CRYPTOGRAPHIC METHODS SHOULD BE DEVELOPED IN RESPONSE TO THE NEEDS, DEMANDS AND RESPONSIBILITIES OF INDIVIDUALS, BUSINESSES AND GOVERNMENTS.

The development and provision of cryptographic methods should be determined by the market in an open and competitive environment. Such an approach would best ensure that solutions keep pace with changing technology, the demands of users and evolving threats to information and communications systems security. The development of international technical standards, criteria and protocols related to cryptographic methods should also be market driven. Governments should encourage and co-operate with business and the research community in the development of cryptographic methods.

This principle embraces the importance of a standard being developed in accordance with market needs. Individuals, business and governments may, however, have irreconcilable needs. The US policy in 1995 sought to promote avoidance of a de facto cryptography standard that did not allow access for law enforcement and national security purposes, but enabled development of global standards which enabled access for these parties.[182] With such a policy, which seems quite irreconcilable, the only alternative is to eschew market-driven development and promote escrowed systems. Hardware escrow systems are preferable since software systems can, after all, be reverse engineered.

The Crisis committee[183] recognized the importance of flexibility in the market and the importance of the market setting trusted standards. One of the Crisis committee's recommendations states. "National cryptography policy affecting the development and use of commercial cryptography should be more closely aligned with market forces".[184]

---

[182] The US Government cryptography policy had in 1995 as its goal to promote the following objectives:

- "Deployment of encryption adequate and strong enough to protect electronic commerce that may be transacted on the future information infrastructure;
- Development and adoption of global (rather than national) standards and solutions;
- Widespread deployment of products with encryption capabilities for confidentiality that enable legal access for law enforcement and national security purposes; and
- Avoidance of the development of de facto cryptography standards (either domestically or globally) that do not permit access for law enforcement and national security purposes, thus ensuring the that the use of such products remains relatively limited."

See Crisis *supra note 67* at 111.

[183] Cryptography's Role In Securing The Information Society (Crisis) See Crisis *supra* note 67

[184] *Ibid* at 305

Strangely the principle itself in the Cryptography Guidelines does not mention market forces, only that cryptographic methods should be developed in response to the needs, demands and responsibilities of a collection of individuals, businesses and governments.[185] One might wonder what the market is if not individuals, businesses and governments. The present wording is indeed open to a wider interpretation and governments can therefore argue that the market alone should not be able to call the tune and that restraints on free choice may be imposed by the government.[186] The principle recognizes that cryptography has become an important part of information security. The explanatory text further expresses the view that development should take place in a open and competitive environment. The word "open" probably refers to a market free from distorted competition. Since the market for information and telecommunication products is growing rapidly, it is essential that governments keeps a technology-neutral approach to cryptographic products, because it is impossible to predict long term developments.

A number of reasons can be put forward why the development of cryptographic systems should be left to the market. Firstly, cryptography policies that are contrary to user need will not be successful in a longer perspective. Secondly aligning with market forces is furthermore probably the most effective way of promoting the use of cryptography.[187] Thirdly, a national cryptography policy that aligns more closely with market forces will allow users to implement cryptographic products that suit their security needs. Law and economic arguments can therefore also be put forward in support for a market force approach. Within such an approach vendors and manufactures will tend to develop different products with different security levels. All users might require maximum-security encryption products. A market force approach may therefore create a more diversified market and spur on further development. A

---

[185] See the "Report on Background and Issues of Cryptography Policy", online: http://www.oecd.org/dsti/iccp/legal/cryptopol.htm, (date accessed 13 November 1997) which mentions that governments may influence product development by expressing needs for certain products and that different views exist. Some believes that governments should guide the market in developing new products in order to protect public safety and privacy. Others believe that governments should refrain from pushing the market in a particular direction.

[186] See "Decoding the OECD's Guidelines for Cryptography Policy", online: http://www.steptoe.com/comment.htm, (date accessed: 11 February 1997)

[187] See Crisis *Supra* at 304 ff This can be done by public procurement and by recognizing standards as Federal Industry Processing Standard (FIPS).

close liaison with the market will also promote the development of new standards. It will be of great importance that governments recognize new standards in close cooperation with the business and research community. Governments should therefore encourage use of cryptographic products that are consistent with industry practice. Governments can promote new emerging standards by adapting them as government standards.[188] Governments will without doubt have to take an active role, but the transition and change will certainly not be easy for many military and governmental agencies that previously have been solely responsible for cryptographic development and see it as their sacred land. Government agencies should moreover support the establishment of new standard-setting bodies and support existent bodies, private as well as public. The standard-setting process should be voluntary, industry-led, consensus-based and international.[189]Standards should, moreover, be open to public scrutiny and not subject to unnecessary security clearances.[190] Another major reason for open standards is user trust. If users feel that they cannot trust the products they will refrain from implementing them. This would be detrimental for any national cryptography policy that has as it's goal to promote – at the very least – the domestic use of encryption.

6.4.4 STANDARDS FOR CRYPTOGRAPHIC METHODS

TECHNICAL STANDARDS, CRITERIA AND PROTOCOLS FOR CRYPTOGRAPHIC METHODS SHOULD BE DEVELOPED AND PROMULGATED AT THE NATIONAL AND INTERNATIONAL LEVEL.

In response to the needs of the market, internationally-recognised standards-making bodies, governments, business and other relevant experts should share information and collaborate to develop and promulgate interoperable technical standards, criteria and protocols for cryptographic methods. National standards for cryptographic methods, if any, should be consistent with international standards to facilitate global interoperability, portability and mobility. Mechanisms to evaluate conformity to such technical standards, criteria and protocols for interoperability, portability and mobility of cryptographic methods should be developed. To the extent that testing of conformity to, or evaluation of, standards may occur, the broad acceptance of such results should be encouraged.

---

[188] In the USA the Clinton administration made an unsuccessful attempt to introduce the Clipper ship through the public procurement power with support of Federal Processing Standards (FIPS)

[189] Report on Background and Issues of Cryptography Policy *supra* note 151, online: http://www.oece.org/dsti/iccp/legal/cryptpol.htm (date accessed 22 October 1997)

[190] One of the major reasons behind the licensing arrangements in the USA is to give the US government an opportunity to learn more about cryptographic products and to learn more about their capabilities. See Crisis *supra* note *66*at 114.

The principle itself does not give much guidance about how national and international standards should be encouraged and established. [191] Considering the global nature of information data flows and financial markets it will be more difficult to agree upon an international standard than a national.[192] Which system that will develop as a standard is difficult to predict, because several different factors will determine the system which becomes a standard.[193] Standards for cryptographic methods may emerge as a de facto standard, through market dominance or through national or international standard-setting bodies. More often than not international standards emerge as de facto standards rather than through international negotiations.[194] The explanatory text emphasizes that national standards should be consistent with international standards. A fundamental problem is, however, that different national views on cryptographic policy makes it hard to develop international standards. An emerging standard that is not in line with a national cryptographic policy risks being rebutted. This was the case with the digital

---

[191] Standards- "An acknowledged measure of comparison for quantitative or qualitative values; a criterion" (The American Heritage Dictionary of the Language, 3rd Ed., (Houghton: Mifflin Company, 1992)

[192] By using standards it is not necessary to have conversion programs or gateway services that slows down operation. See "Towards An European Framework for Digital Signatures and Encryption, online: http://www.ipso.cec.be/eif/policy/97503.html, (date accessed: 2 November 1999) at 19 [hereinafter *Towards an European Framwork*]

[193] For a time three video standards competed for example. These standards were; Betamax, Video C and VHS. Finally VHS emerged as a de facto standard, despite the fact that many experts considered Betamax to be a better standard. The product developer that can present a product before any competitors and get a large market share has a great chance to be able to set a de facto standard. Microsoft, which has a market share of about 80 percent, can more a less set a standard for all other software developers to follow. During the last 10 years there has been a tendency, particularly in the computer and telecommunication markets, to develop open standards rather than proprietary ones. The advantage with an open standard is that it will be accepted more easily and therefore established earlier. Instead of making profit on royalty producers can achieve larger market share and sell more products.

[194] One example of a national cryptographic standard that has become an international de facto standard is the Data Encryption Standard (DES). DES is a cryptographic method developed by the IBM in the 1970s. DES was later accepted by the National Bureau of Standards (NBS) in the USA (Now National Institute of Standards and Technology) in competition with several other methods as a Federal Information Processing Standard (FIPS). The DES has become a de facto standard today in the financial market, but DES is getting increasingly easy to break with today's more powerful computers. The acceptance of the DES sparked an international interest in cryptography and promoted use of cryptography. The National Security Agency (NSA) which saw cryptography as within their domain did not appreciate the development of the DES. In 1987, when the Computer Security Act (Public Law 100-235) was promulgated, NIST was vested with the authority of approving cryptographic standards. A memorandum of understanding and agreement (MOU/MOA) was later signed between the NSA and the NIST. One of the major objectives behind the MOU/MOA was to avoid double work. The agreement has, however, been criticized for transferring power from NIST to NSA. See *Privacy on the Line supra* note 29at 68-69. For a background to the DES see further D.K. Branstad, ed., *Computer Science and Technology. Computer Security and the Data Encryption Standard, Proceedings of the Conference on Computer*

signature standard in the USA. RSA[195] (Rivest, Shamir, Adelman) had developed a digital signature algorithm that had become more or less a de facto standard. It was, however, never accepted as a federal standard, because the algorithm could with relative ease be used for confidentiality purposes as well. If an international standard is going to succeed it has to be based on a trusted cryptographic method.[196]

The only way to achieve an international key recovery standard, as has been proposed by the USA, will be through negotiation. An international standard that is not tied to some sort of key escrow key recovery system will on the other hand have a greater chance to get accepted. So far, despite intensive lobbying by the US Government, there has not been an international acceptance of key recovery or key escrow systems. This is probably largely due to fear of loss of keys and disagreement regarding storage of the keys. Not many countries would accept that sensitive keys to key business in their country would be stored elsewhere than within the country. International cooperation will be necessary to agree on international standards. The OECD Council stresses, in the explanatory text, that the needs of the market should steer collaborations and promulgation of standards.[197]

Why is it so important to collaborate?

Today, even though many communication systems are based on open standards, these systems do not interoperate without difficulties. Non-open or proprietary standards would increase these difficulties further. Difficulties in making systems interoperable will be doubled if cryptographic standards are not specified. For full interoperability and seamless international communication networks it is therefore essential to have cryptographic standards.[198] Only when a standard fully specifies how keys should be

---

Security and the Data Encryption Standard, (Washington D.C, U.S Government Printing Office, 1978) (CNBS SP500-27)

[195] See "RSA Security" (18 August 2000) Http://www.rsa.com (date accessed: 18 August 2000)

[196] DES has become a standard despite allegations about a backdoor to the algorithm in the so-called S-boxes. Other cryptographic standards introduced in the United States after the DES has not been very successful, largely because of lack of trust. For a critical review of the Escrowed Encryption Standard (EES) FIPS 185 and the Digital Signature Standard (DSS) FIPS 186 see S. Landau et al., *Codes, Keys and Conflicts,* (Washington D.S. Association for Computing Machinery Inc., 1994) at 48 and 41 respectively. [hereinafter *Codes, Keys and Conflicts*]

[197] See the earlier discussion about the interpretation of the market under the previous principle.

[198] Protocol negotiation is a method gaining more and more attention among product developers. By mutually negotiating, a protocol devices may be freed from having to conform to a single standard. By

exchanged, data streams formatted and cryptographic algorithm used, will different cryptographic standards be fully interoperable.[199] An effective standard-setting process should therefore be industry-led, voluntary, consensus-based and international.[200]

Which Are The International Recognized Standard Making Bodies That should Collaborate?

Some international standard making bodies that can contribute in the international standard-setting process are the International Standardization Organization (ISO) the International Telecommunication Union (ITU-T) (X500 and ISO9594), IEC, the Internet Engineering Task Force (IETF) (public key infrastructure) and the World Wide Web Consortium (W3C) (W3C Digital Signatures Initiative). However, as Mr. Nigel Hickson who led the discussion on standards for cryptographic methods in the Emerging Market Economy Forum (EMEF) workshop pointed out, it is very important that industry develop standards such as the SET (Secure Electronic Transactions) protocol.[201] The European Commission encouraged in 1997 industry and international standardization organizations in the Bonn Ministerial Declaration to develop international standards to ensure secure and trustworthy use of networks.[202]

Keywords for an International Standard;[203] Interoperability, Portability And Mobility

An international standard should specify the criteria under which different cryptographic systems should work together i.e. **interoperability**, criteria for **portability** i.e. a protocol for how cryptographic systems should function on different platforms or operating systems and finally **mobility,** the ability by cryptographic systems to operate in different infrastructures and countries.[204] Management standards

---

negotiating protocols older standards can be supported as well. Extensive protocol negotiation will, however, affect performance. See Crisis *supra* note 67 at 71)

[199] *Ibid* at 71

[200] See Report on Background and Issues of Cryptography Policy, *supra* note 131 at 5

[201] OECD, General Secretariat, Liaison and Co-Ordination Unit, Committee for Information, Computer and Communication Policy, OECD Emerging Market Economy Forum, *Report On The Workshop On Cryptography Policy*, SG/EMEF/ICCP (98)1, (Paris December 1997) at 13 [hereinafter *OECD Cryptography Workshop*]

[202] See Towards An European Framework *Supra* note 192 at 20

[203] For a general background to standards see C. F. Cargill, *Information, Technology & Standardization* (Bedford, Massachusetts: Digital Press, 1989) at 213

[204] **Portability** is defined as "...the technical ability to be adopted and function in multiple systems.

moreover have to be developed for CAs and technical standards for notably digital signatures and certificate formats.[205]

The role for governments

Governments can play an important role not only for the development and evaluation of standards, but also for consolidating emerging standards. The European Commission launched new projects within the 5th Framework Program (1998 – 2002) focusing on Electronic Commerce and notably interoperability and privacy in order to stimulate interoperability and widescale deployment of standards.[206]

Development and evaluation of new standards

Governments have an authoritative position in the development of standards. Criteria and evaluation of new standards are often made through governmental agencies that usually have better resources at their disposal than the private sector. Testing for conformity against standards will allow users to evaluate effectiveness of different cryptographic methods and products. This will be important particularly in the field of public key authentication since cross certification is an essential element of authentication.[207] Government bodies can also be assumed to be more objective in their evolution of products and methods.[208] One potential source of problems for governmental agencies is that they so far have been more directed towards developing cryptographic methods for the public sector, in particular for military defense purposes. The need of the private market and of the private sector differ from the needs of the public sector in many respects.[209]

Interoperability is defined as "...the technical ability of multiple cryptographic methods to function together."
Mobility is defined as "...technical ability to function in different countries or information and communication infrastructures."

[205] See Towards An European Framework *supra* note 192 at 20.

[206] See Towards An European Framework at 20. The 5th Framework Program is intended to put together a common framework for cryptography throughout the European Union during 1998 – 2000.

[207] See Orlowski *supra* note 165 at 4

[208] One problem with letting national security agencies do evaluation of cryptographic methods is that such testing will reveal the level of knowledge that the national security agency poses.

[209] The Crisis Committee concluded in the report; "How useful such technologies will prove for corporate information remains to be seen. Increasing needs for information security in the private sector suggest that NSA technology may have much to offer, especially if such technology can be made available to the

Governments have, moreover, an important role to play in consolidating standards through their procurement powers.[210] The acceptance of a standard by a government leads to a "seal of approval" that the standard has been thoroughly tested. Bulk purchases by governments can, furthermore, consolidate standards since producers can cover research and development costs faster. Once a break-even point has been reached for a product the price for the product can be lowered. A low price will make the product more attractive and through increased sales greater market share can be achieved. Government procurement can therefore enhance scale production and is of great importance for standard setting.

Intellectual property rights and standards

Intellectual property rights may obstruct the development and use of cryptographic methods. The widespread use of DES is probably partly a result of DES being an open standard. International Business Machines (IBM) granted a non-exclusive royalty-free license to make, use and sell apparatus that complied with the standard.[211] DES has today become a de facto standard. The RSA's Digital Signature Standard algorithm had the status of a de facto standard in the United States. Despite that, the RSA algorithm was rejected as a federal standard on the basis that it could easily be used for confidentiality purposes as well. Another reason why it was rejected was that RSA Inc. had patented the algorithm and royalties would therefore have to be paid to the RSA, thereby making the standard more expensive.[212]

---

private sector without limitation. At the same time, the environment in which the private sector information security needs are manifested may be different enough from defense and foreign policy needs. These technologies may not be particularly relevant in the private sector. Furthermore may the rapid pace of commercial developments in information technology make it difficult for the private sector to use technologies developed for national security purposes in a less rapidly changing environment. (Crisis *supra* note 67 at 228)

[210] The failed attempt by the Clinton administration to introduce the Clipper chip with the Skipjack algorithm shows however, that use of governmental procurement can backfire if the standard is not trusted and does not have public support. Governmental procurement power should therefore be used with caution.

[211] Crisis *supra* note 67 at 222

[212] The main reason behind the decision not to accept the RSA Digital Signature Standard was that widespread adoption of the algorithm could result in an infrastructure for easy distribution of DES keys. (See Crisis *supra* note 67 at 222 and further US, Office of Technology Assessment, *Information Security*

6.4.5 PROTECTION OF PRIVACY AND PERSONAL DATA[213]

THE FUNDAMENTAL RIGHTS OF INDIVIDUALS TO PRIVACY, INCLUDING SECRECY OF COMMUNICATIONS AND PROTECTION OF PERSONAL DATA, SHOULD BE RESPECTED IN NATIONAL CRYPTOGRAPHY POLICIES AND IN THE IMPLEMENTATION AND USE OF CRYPTOGRAPHIC METHODS.

Cryptographic methods can be a valuable tool for the protection of privacy, including both the confidentiality of data and communications and the protection of the identity of individuals. Cryptographic methods also offer new opportunities to minimise the collection of personal data, by enabling secure but anonymous payments, transactions and interactions. At the same time, cryptographic methods to ensure the integrity of data in electronic transactions raise privacy implications. These implications, which include the collection of personal data and the creation of systems for personal identification, should be considered and explained, and, where appropriate, privacy safeguards should be established.

The OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data provide general guidance concerning the collection and management of personal information, and should be applied in concert with relevant national law when implementing cryptographic methods.

Under this heading the council refers to an earlier adopted recommendation:

The reason for this is that these guidelines for privacy protection have been recognized internationally

> "In adopting these Guidelines, the OECD Member Countries clearly intended to "help to harmonise national privacy legislation and, while upholding such human rights, to prevent at the same time interruptions in the international flow of data".
> Since then [the adoption], the Recommendation has proved to represent international consensus on general guidance concerning the collection and management of personal information. The principles contained in the OECD Privacy Guidelines are reflected in legislation and practices for the protection of privacy world-wide. Moreover, theses principles were designed in a technology neutral way to accommodate future developments: they are still applicable with regard to any technology used for collecting and processing data, including network technologies."[214]

Indeed the OECD Privacy Guidelines have been a success in terms of international recognition. However, what we have achieved over the last 18 years at an international

---

And Privacy in Network Environments, OTC-TCT-606, US Government Printing Office, Washington D.C., 1994 ff. 167 and 217 ff

[213] Privacy in an electronic environment has been dealt with earlier under the heading Privacy in part II. In this part privacy in relation the work done by the OECD and in close relation to the OECD Cryptography Policy Guidelines are dealt with.

[214] "Privacy Protection on Global networks", online: http://www.oecd//dsti/sti/it/secur/act/privnote.htm., (date accessed : 1 November 1998) at 1

level has not been encouraging.[215] Fear of privacy intrusion has certainly not diminished. On the contrary it has grown. Privacy in the electronic environment is fundamental for the development of the information society and the right to privacy has been recognized as a human and fundamental right. Despite international recognition, the implementation of the OECD Privacy Guidelines has been poor. The focus has been much more on maintaining an uninterrupted flow of data than a thorough implementation of the OECD Privacy Guidelines for the sake of privacy itself.[216] The OECD has in recent years recognized that more work needs to be done on the international level and has launched a plan to overcome the lack of privacy in electronic environments. What the OECD has done so far will be dealt with later. Let us first look at the OECD Privacy Guidelines and the OECD Cryptography Policy Guidelines that these are intended to be applied in concert with.

The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

The Privacy Guidelines were adopted as a Recommendation of the OECD Council in September 1980. They were drafted to be technology neutral and were intended to give general guidance concerning the collection and management of personal information for both the public and the private sector. The draft was based on common values derived from the outwardly divergent approaches taken by the Member countries and represented advanced or consolidated ideas about privacy protection.[217]
The four recommendations were:

1. That Member countries take into account in their domestic legislation the principles concerning the protection of privacy and individual liberties set forth in the Guidelines contained in the Annex to this Recommendation which is an integral part thereof;

---

[215] See the statement by David Chaum *supra* note 99 under Privacy in part II.
[216] One of the main ideas behind the OECD Privacy Guidelines when they were drafted in the end of the 1970s was to prevent legal issues concerning privacy from creating obstacles to economic and social relations. See OECD, "Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet (DSTII/ICCP/REG(97)6/FINAL) at 5
[217] By the time the Privacy Guidelines were adopted privacy legislation had already been introduced in Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States. See the preface to the OECD Privacy Guidelines. *infra*.

2. That Member countries endeavour to remove or avoid creating, in the name of privacy protection, unjustified obstacles to transborder data flows of personal data;
3. That Member countries co-operate in the implementation of the Guidelines set forth in the Annex;
4. That Member countries agree as soon as possible on specific procedures of consultation and co-operation for the application of these Guidelines.[218]

The OECD Privacy Guidelines themselves are divided into four parts; I General, II Basic principles of national application, III Basic principles of international application: Free flow and legitimate restrictions, IV National implementation and international co-operation. An explanatory memorandum is attached to the recommendations. The purpose of the memorandum is to provide a background to the issues dealt with in the principles. Application of the Guidelines are limited to "personal data, whether in the public or private sectors, which, because of the manner in which they are processed, or because of their nature, or the context in which they are used, pose a danger to privacy and individual liberties".[219] Personal data is defined as "any information relating to an identified or identifiable individual (data subject)." A rather surprising limitation is found in the Scope of the Guidelines under paragraph 3 c); "These Guidelines should not be interpreted as preventing the application of the Guidelines only to automatic processing of personal data".[220] How automatic processing of data should be defined is, however, left open to interpretation. The manner in which the Privacy Guidelines have been drafted reoccurs in the Cryptography Policy Guidelines and can be criticized as being too vague. The guidelines are not authoritative enough in themselves to support harmonization.

The OECD Privacy Guidelines consist of a number of principles followed by more detailed guidelines. The scope of the Guidelines contains however so many exclusions and ambiguities that the guidelines become watered down as a result. For the scope of the Cryptography Policy Guidelines the Security Safeguards principle is of special interest because cryptography represents the best method to protect data against unauthorized access, risks and losses. It is, moreover implicit in this principle that

[218] OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data of 23 September 1980 [C80 58 Final]
[219] *Ibid*

Member countries have a duty to take all reasonable and appropriate steps to ensure that transborder flows of personal data are uninterrupted and secure. This is an aim that will require international co-operation among the Member countries to achieve. The most promising and efficient method to secure transborder flows of data is cryptography.[221] As shown there are very close links between the Cryptography Guidelines and the Privacy Guidelines.

Protection of Privacy and Personal Data in the Cryptography Guidelines

The council uses the word "fundamental" and thereby reaffirms the right to privacy, a right that has become increasingly important over the last hundred years because of new technological developments.[222] It is important to note that the Guidelines only mention individuals. Confidentiality in business transactions is not covered by the Cryptography Guidelines. It is neither a fundamental nor human right, even though the opposite has sometimes been argued. The right to privacy is related to individuals and cannot in my

---

[220] *Supra* note *218 at 2*

[221] Paragraph 17 allows Member countries to restrict transborder flow of data. This has been a considerable debate since the European Union passed a database directive that requires adequate protection in third countries over this issue. Hopefully, the EU Database directive will put some pressure on the countries that have not fully implemented the OECD Privacy Guidelines yet. The United States has for a long time tried self-enforcement with little success. See further "Pretty Poor Policy", Wired (28 June 1998), online: http://www.wired.com/news/politics/story/13256.html for a critical review of the policy.

[222] One of the earliest historical sources where privacy is mentioned is in the Talmud, and the right to privacy therefore dates more than 2000 years back. In the Talmud the right to privacy, or rather obligation to show privacy, was mentioned as a right towards the neighbors; a neighbor should not peer and look into another neighbor's house. See H. Danby, *The Misnah* (Oxford: Oxford University Press, 1933) at 367. In the United States where the right to privacy from Government intrusion has been very much debated because of the Clipper chip initiative privacy has been recognized more than several hundred years. According to L Friedman, *A history of American Law* (New York: Simon and Schuster, 1973) at 275, the early colonists in the United States applied English law, that by that time, provided for punishment of eavesdroppers.
Internationally, the right to privacy has been recognized since the passing of the Universal Declaration of Human rights in 1948, which in article 12 reads; "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks".
The wording is reiterated in the 1967 International Convenant on Human Rights with a minor editorial difference. (The paragraph is divided into two articles instead of one.) The right to privacy is fundamental in a democratic society and the right to privacy is one of the first rights lost when a dictator is getting power. Widespread and exhaustive surveillance of the citizens is, in fact, a characteristic of totalitarian regimes. The use of informers (human intelligence), electronic surveillance (signals intelligence) and other watchdogs has always been a tool to control and suppress opposition. There are several examples of totalitarian regimes where privacy not have been respected for example Romania and East Germany, or is, respected, for example Syria or China.

view pertain to entities.[223] The Cryptography Policy Guidelines represent an extension of the rights of individuals in that respect because they are not only limited to personal data, as are the Privacy Guidelines. There is no definition of the concept of privacy but according to the explanatory text it includes at least secrecy of communications and protection of personal data.

The right to secrecy in communications contra government surveillance

The right to secrecy in communications goes one step further than the Privacy Guidelines and it seems to be presented as an absolute right at first glance. It is, however, stated in the Cryptography Policy Guidelines that no principles are interdependent and that no principles should be interpreted in isolation. That the Guidelines do not apply to what are considered national security interests has been observed earlier. The question thus emerges as to what extent secrecy in communications actually is protected. If the principle of privacy is applied in concert with the principle of lawful access we can conclude that the principle of privacy has to be respected to the greatest extent possible.

According to the Cryptography Policy Guidelines a requesting authority has to have a legal right to the encrypted data. Moreover, information so obtained can only be

---

[223] For a more philosophical and fundamental review of privacy see A. L. Allen, *Uneasy Access:Privacy for Women in a Free Society* (Rowman and Littlefield, 1995), R. Dworkin, *Life's Dominion, An argument about Abortion, Euthanasia, and Individual freedom* (New York: Alfred A. Knopf, 1993), A.F.Westin, *Privacy and Freedom,* (Athenum, 1967) F. D.. Schoeman ed., *Philosophical Dimensions of Privacy: An Anthology* (Cambridge, Massachusetts: Cambridge University Press, 1984) For a more investigate review of privacy and computers see D. Burnham, *The Rise of the Computer State* (New York:Random House, 1983) R. E. Smith, *How to protect Privacy- What's Left of It* (New York: Anchor Press, 1979) More conceptual studies privacy are the works by D.Lyon and E. Zureik, eds., *Computers, Surveillance, and Privacy* (Minneapolis: University of Minnesota Press, 1996).
Some comparative studies that deserves to be mentioned are the works by C. Bennett, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992), D.H. Flaherty, *Protecting Privacy in the Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States* (Richmond: University of North Carolina Press, 1989) and A.C.M. Nugter, *Transborder Flow of Personal Data within the EC: A Comparative Analysis of the Private Statutes of the Federal Republic of Germany, France, the United Kingdom and the Netherlands* (Antwerpen: Kluwer, 1990). Two studies that comes close to the conceptual study in this thesis are the work by J. H. Smith, *Managing Privacy: Information Technology and Corporate America* (Chapel Hill: University of North Carolina Press, 1994) about organizational problems and the work by P. M. Reagan, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press, 1995)

used in accordance with the law[224] The process through which the cryptographic keys are obtained shall, furthermore, be recorded in order to allow audit as to whether the actions were lawful. The duration of the surveillance has, moreover, to be limited to what is "appropriate".[225]

According to the explanatory notes cryptography can be used both to protect personal data, but at the same time can raise privacy implications. It is not really evident what is meant. Probably the establishment of Certification Agencies (CAs), or Trusted Third Parties (TTPs) as they are sometimes called, is what the drafters had in mind. As has been described earlier in part II under Cryptography Techniques and Methods, a problem with the use of public key cryptography is the identification of the cryptographic key holder. How can it be established that the issuer of the key is who he alleges he is? Two principal solutions exist. Both have disadvantages. With PGP (Pretty Good Privacy), a web of trust is created, i.e. one user validates another user. Alice might for example know Bob and can therefore verify for Charlie that the key he has got originates from Bob. This web of trust is easy to handle on a small scale. In a larger group it becomes unfeasible.

A possibility might be to establish a hierarchical structure like the X509 structure[226]. How this structure should be established is a widely debated issue. In any such structure the CAs have to confirm that certain personal identificators connected

---

[224] This provision stipulates what the surveying entities are allowed to do with surplus information. Surplus information has to be deleted in order to comply with the principle. When the information is not relevant to an ongoing investigation, the principle of privacy and protection of personal data overrides the principle of lawful access.

[225] Several questions and concerns can be raised in relation to lawful access to cryptographic keys and to privacy. According to the explanatory text, privacy safeguards should be established where appropriate. It is therefore reasonably to assume that the designated time for surveillance should be limited to what is appropriate. It would, however, have been preferable if the guidelines had stated that access to cryptographic keys has to be time-limited. It seems quite difficult to determine what "appropriate" refers to. Another issue is who will determine what is appropriate? A Guideline that leaves so much room for the Member states to interpret does not give much guidance. It certainly does not provide much harmonization. What causes even more concern is how cryptographic keys should be returned. Cryptographic keys are, after all, not like ordinary keys. Once obtained a law enforcement agency will have access to the keys until the user changes the keys. The key is just a file that easily can be stored or – forgotten to be deleted. A major concern is therefore that surveillance is never terminated. It is therefore in my view essential to have a system of checks and balances to make sure that the keys are deleted. The keys can be kept so easily that the risk of misuse is evident. One safeguard might therefore be an obligation for the authority to reveal to the individual that surveillance of him has taken place. The revelation that he or she has been under surveillance might otherwise result in such a change in behavior and procedures by the individual that render further surveillance impossible.

with the cryptographic keys are correct and thereby confirm that the user is the rightful owner of the keys. The greater the demand for identification, the more privacy concerns emerge, because the more personal data is needed to make a reliable identification. The databases containing all this personal information are going to be extremely sensitive. The protection of such information will give rise to difficult liability questions.[227]

Ongoing developments

Privacy protection is of great and growing concern for consumers in a knowledge-based economy. The protection of privacy in a networked environment is, as described in part III, closely related to the use of cryptography. Within the OECD, work is ongoing in the area of privacy protection. One of the conclusions of the OECD Conference "Dismantling the Barriers to Global Electronic Commerce" held in Turku, Finland was that privacy protection is a *sine qua non* condition for the development of electronic commerce.[228] At the OECD Ministerial level Conference "A Borderless World: Realising the Potential of Global Electronic Commerce held in Ottawa, Canada 7-9 October 1998, protection of privacy was one of the main issues. The report "Implementing the OECD Privacy Guidelines in the Electronic Environment: Focus on the Internet" had three major proposals to OECD Member States Governments;

- reaffirm that the Privacy Guidelines are applicable with regard to any technology used for collecting and processing data;
- encourage those businesses that choose to expand their activities to information and communication networks to adopt policies and technical solutions which will guarantee the protection of the privacy of individuals on these networks, particularly on the Internet;
- foster public awareness and education on issues related to protection of privacy and the use of technology.[229]

---

[226] A ITU standard for a worldwide directory standard. X509 is the part that pertains to Public Key Infrastructures. (PKI)

[227] See further under the liability principle in Part VI

[228] "Privacy protection on Global Networks", online: http://www.oecd.org//dsti/sti/it/secur/act/privnote.htm (date accessed 4 August 1998).

[229] *Ibid.* It is, of course, natural to build on previous work, such as the OECD Privacy Guidelines. There is is, however, a danger in reaffirming the Guidelines. It is the implementation of the Privacy Guidelines that has been poor. New more comprehensive implementation is required, a result that can only be achieved by an international consensus because of the increasingly international nature of data flows. More effective sanctions are also required. The European Union's data base directive will probably be of more importance for international privacy protection because of the tougher sanctions. The risk that European Union Member States prohibit re-export of data has already caused a lot of stir in several countries. In Canada it has been a major reason to look over personal privacy protection.

Another difficulty is the various approaches to privacy protection in the OECD Member countries. The United States of America has, not surprisingly, chosen a more market-based approach with greater emphasis on self-regulation than the European countries, even though it seems that the Clinton administration is starting to lose patience with the state of the current self-regulation structure.[230] Based on the above mentioned report a workshop was initiated with the support of the Business an Industry Advisory Committee (BIAC) on 16-17 February 1998.[231] The participants in the workshop recognized that electronic commerce requires increased consumer confidence in privacy protection. The participant representatives from governments, the private sector user and consumer communities, reaffirmed that the Privacy Guidelines continue to provide a common set of fundamental principles.[232] The chair Michelle D'Auray noted that a balance has to be struck between the benefits of free flow of information and on-line personal privacy protection. She concluded that to achieve the balance the following requirements had to be met; "education and transparency, flexible and effective instruments; full exploitation of technologies and enforceability and redress".[233] Cryptography enhances all these qualities and possibilities. The chair furthermore emphasized the need to survey all possible instruments for privacy protection (including law, self-regulation, contracts and technology). The purpose of the proposed study would be to identify gaps and barriers to interoperability, redress coverage across jurisdictions and furthermore, to suggest possible solutions for a seamless international privacy protection.[234] Such a study is currently under way.[235]

---

[230] See "Pretty Poor Privacy", http://www.wired.com/news/news/politics/story/13256.html, (date accessed: 28 June 1998).

[231] "Workshop on Privacy Protection in a Global Networked Society", http://www.oecd.org//dsti/sti/it/secur/prod/reg98-5 final.pdf, (date accessed: 12 September 1998) at 6 The workshop addressed four issues that could be implemented irrespective of the different approaches;

- "identifying and balancing the needs of the private sector and those of users and consumers and formulating efficient strategies for "educating for privacy";
- developing "privacy enhancing technologies";
- implementing enforcement mechanisms developed in the private sector for privacy codes of conduct and standards;
- adopting a model contractual solutions for transborder data flows"

[232] *Supra* note 231 at 7

[233] *Ibid* at 7

[234] *Ibid* at 7

[235] *Supra note* 214 at 3

The Group of Experts on Information Security and Privacy, another expert group within the OECD, held a meeting the 18-19 May 1998 at which the 1980 OECD Privacy Guidelines were reaffirmed. Moreover, a statement was issued that privacy protection requires greater attention in network technologies. The Group also emphasized that countries should make greater efforts to implement the OECD 1980 Privacy Guidelines.[236]

6.4.6 LAWFUL ACCESS

NATIONAL CRYPTOGRAPHY POLICIES MAY ALLOW LAWFUL ACCESS TO PLAINTEXT, OR CRYPTOGRAPHIC KEYS, OF ENCRYPTED DATA. THESE POLICIES MUST RESPECT THE OTHER PRINCIPLES CONTAINED IN THE GUIDELINES TO THE GREATEST EXTENT POSSIBLE.

If considering policies on cryptographic methods that provide for lawful access, governments should carefully weigh the benefits, including the benefits for public safety, law enforcement and national security, as well as the risks of misuse, the additional expense of any supporting infrastructure, the prospects of technical failure, and other costs. This principle should not be interpreted as implying that governments should, or should not, initiate legislation that would allow lawful access.

Where access to the plaintext, or cryptographic keys, of encrypted data is requested under lawful process, the individual or entity requesting access must have a legal right to possession of the plaintext, and once obtained the data must only be used for lawful purposes. The process through which lawful access is obtained should be recorded, so that the disclosure of the cryptographic keys or the data can be audited or reviewed in accordance with national law. Where lawful access is requested and obtained, such access should be granted within designated time limits appropriate to the circumstances. The conditions of lawful access should be stated clearly and published in a way that they are easily available to users, keyholders and providers of cryptographic methods.

Key management systems could provide a basis for a possible solution which could balance the interest of users and law enforcement authorities; these techniques could also be used to recover data, when keys are lost. Processes for lawful access to cryptographic keys must recognise the distinction between keys which are used to protect confidentiality and keys which are used for other purposes only. A cryptographic key that provides for identity or integrity only (as distinct from a cryptographic key that verifies identity or integrity only) should not be made available without the consent of the individual or entity in lawful possession of that key.

The Balancing Act

According to this principle national cryptography policies may allow lawful access to plaintext or cryptographic keys.[237] The explanatory text states that the principle should

---

[236] "Work in Progress", online: http://www.stategis.ic.gc.ca/ottawaoecdconfernece/ott_wip.htm , (date accessed: 27 October 1998)

[237] It is worth noting that access to plaintext is mentioned first. This is, of course, not a coincidence; The risk of misuse is considerably smaller if access to plaintext is given rather than access to cryptographic keys. Someone with access to signature keys might inpersonify the rightful owner of the keys. To rebut any transaction made using someone's signature keys will be extremely difficult since there is a presumption that the rightful owner and only the rightful owner has access to the keys. That is the base for the reliability of digital signatures. If that assumption cannot be trusted the whole system will break down. That is why the concept of trust is so important.

not be interpreted as implying that government, should (or should not) initiate legislation to allow lawful access. According to the explanatory text, a balanced approach should be taken towards adopting any restrictive measures in the name of encryption. In my view the principle should be interpreted so that as law enforcement agencies should only have access to cryptographic keys if access to plaintext would not be sufficient. It may for example be necessary to obtain information in real time. The principle itself states that the other principle- of trust, choice, market-driven development, standards and privacy-should be respected to the greatest extent possible. The principle reveals one of the fundamental questions that have caused debate: whether a key access system should be adopted or whether a more market-based approach is preferable. Before any such decision is taken a careful consideration of all the interests has to be undertaken, then the interests at stake have to be balanced. The solution is not a compromise. It is a question of adopting either a key access system or a system where the privacy of the individual is paramount. Resulting unbalances have to be subsequently addressed, for example through legislation.

Lawful access to cryptographic keys

How lawful access across national borders is to be achieved is further explained in the explanatory notes of the principle on International Co-operation, which states that lawful access should be achieved through bilateral and multilateral agreements. It will not be an easy task to negotiate such bilateral or multilateral agreements for a number of reasons. One reason is that the right to privacy is enumerated as a fundamental right in the Cryptography Policy Guidelines as well as in most democracies. To balance privacy with other interests will be politically sensitive and cause public debate. Will a government hand over cryptographic keys belonging to one of its citizens to a foreign government? To what extent can, for example, law enforcement agencies use surplus information obtained with the help of the keys? If a state implements a key escrow system or a key recovery system it might have to hand over cryptographic keys to another state. By doing so the state loses control of how the keys are then used. If for example a country's wiretapping law allows wiretapping in cases where a suspect may be imprisoned for more than 10 years and the country uses the key for other purposes

and less severe crimes, can the citizen whose privacy has been infringed then sue for damages? Doubtlessly access to cryptographic keys over national borders has to be subject to careful consideration. Agreements regarding access to plaintext will probably be easier to negotiate since similar agreements already exist regarding co-operation. A country that hands over the documents will keep control of the information that has been accessed. This is not the case with handing over cryptographic keys.

Key management systems

In the third section in the explanatory text guidance for policies regarding key management systems is given. The term key management is used in the explanatory text in a much broader sense than usually used in the doctrine. It is suggested in the explanatory text under the principle of Lawful access, that if a key management system is established, it should balance interests of users as well as those of law enforcement agencies. No explanation as to how this should be achieved is, however, provided. One possible interpretation is that governments should have access to the keys through a key management system such as a certification agency, which then would hold the private keys. Such a system might result in CAs' incurring liability for damages if keys are compromised. Inevitably, keys will be lost and a system for revocation of keys will therefore be necessary. No guidance how such a system should be constructed is given in the explanatory text, only that key management systems should use the same techniques to recover data when keys are lost. Systems for revocation of keys need to be on-line so that a key that has been compromised can be revoked immediately.

Judicial concern of lawful access to cryptographic keys

Another important issue is judicial control over cryptographic keys, which have been handed over to law enforcement agencies and national security agencies should be exercised. Once keys have been handed over for law enforcement reasons it will be very difficult for the one , who unjustly has had his privacy infringed, to get rehabilitation.

The explanatory text states that the process through which lawful access is obtained should be audited. It should be possible to identify who has had access to the keys. Even if someone finds out that his keys have been compromised unjustly through

a lawful access procedure, there will be very little he can do about it. The explanatory text mentions that only designated access to keys should be permitted. Cryptographic keys should for example be deleted once the investigation is terminated. What happens if a secret key is compromised and used by someone else during the period when lawful access to the keys has been granted? Will the owner of the keys then be informed that his keys have been compromised and that he has been under surveillance? If a suspect is told that he has been under surveillance, then he probably will change his behavior considerably. It is, for example, likely that he will change his private key. If the suspect therefore is told that he is under surveillance the whole operation might be in jeopardy. As one can understand there might be considerable negative consequences for an individual if cryptographic keys are compromised without his knowledge and therefore precluding him from remedying the situation. In what follows the related issue of government liability in a key access system is analyzed.

6.4.7 LIABILITY

WHETHER ESTABLISHED BY CONTRACT OR LEGISLATION, THE LIABILITY OF INDIVIDUALS AND ENTITIES THAT OFFER CRYPTOGRAPHIC SERVICES OR HOLD OR ACCESS CRYPTOGRAPHIC KEYS SHOULD BE CLEARLY STATED.

The liability of any individual or entity, including a government entity, that offers cryptographic services or holds or has access to cryptographic keys, should be made clear by contract or where appropriate by national legislation or international agreement. The liability of users for misuse of their own keys should also be made clear. A keyholder should not be held liable for providing cryptographic keys or plaintext of encrypted data in accordance with lawful access. The party that obtains lawful access should be liable for misuse of cryptographic keys or plaintext that it has obtained.

The principle

This principle will be of substantial importance for users. The liability question will, furthermore, be one of the most difficult issues to solve since so many jurisdictions will be involved, which will complicate the matter. The main message the principle puts forward is that liability issues should be clearly stated for the user, no matter if cryptographic services are offered by individuals, businesses or governments. Flaws in

systems and human errors will result in loss of keys and a transparent and trustworthy national and international framework to deal with liability issues will be necessary. Liability issues can emerge in several situations.

Obligations to adequately protect data

Legislation or standards of conduct may require business, public authorities and individuals to maintain adequate protection of information systems.[238] Cryptography is one way to protect sensitive information. Use of cryptography might, however, also incur liability. I will start with giving some examples of when cryptography can be used and perhaps should have been used to protect data. I will thereafter try to analyze some situations in which liability might be incurred.

Business

Some reporters that wrote about hackers discovered that their telephone calls were being forwarded to other locations where the callers were greeted with obscenities. Their e-mail boxes were, furthermore, filled with junk e-mail.[239]

Governments

In at least two instances inmates have been able to forge public information. In the first instance an inmate managed to alter his release date on the on-line prison information system. The attempt failed, however, when a suspicious deputy checked the manual entry after the inmate had been bragging about his impending release.[240] In another case a forger was released too early after an authentic fax was received by the jail ordering his release.[241] In several countries there is a duty on authorities and private entities to

[238] From 1989 to 1992, 45 Los Angles police officers were cited for using department computers in an unauthorized manner to run background checks for personal manners. See Neumann, *Computer-Related Risks*, 1 November 1992 at 184. One of the most well known interceptions of telecommunications is the overheard conversation between princess Diana and a man who called her "my darling Squidge". The conversation was taped by an individual and published in the Sun. See Neuman *ibid* at 186 and further J. Flinn, *San Francisco Examiner*, (1 November 1992).

[239] P. Elmer-Dewitt "Terror on the Internet", *Time*, (12 December 1994) at 73

[240] *San Jose Mercury News*, 14 December 1984.

[241] *San Francisco Chronicle*, "Fraudulent Fax Gets Forger Freed", (18 December 1991) at 3

protect confidential information from being accessed by unauthorized persons.[242] Directive 95/46 EC, on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data states for example:

> "Article 17
>
> Security of processing
>
> 1. Member States shall provide that the controller must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing."
>
> Having regard to the state of the art and the cost of their implementation, such measures shall ensure a level of security appropriate to the risks represented by the processing and the nature of the data to be protected.[243]

According to the article Member States have an obligation to ensure and enforce that the controller, or the processor carrying out the processing on his behalf, can provide sufficient technical and organizational security guarantees.

Individuals

There might, moreover, be a duty also on the part of individuals to exercise due diligence to protect data that they have in their possession.[244] In 1994 a bounty of

---

[242] In the Swedish "Datalagen (SFS 1973:289)" Section 6 para 10 control and security are mentioned as two issues that the responsible Swedish authority "Datainspektionen" may issue conditions on in personal registers. The entity having a personal register has to observe that no unauthorized access or alteration is being done. See 7 § of the Swedish "Datalag". (The Swedish Datalag was replaced by The Personal Data Act "Personuppgiftslag" (SFS 1998:204) on 24 October 1998)

[243] EC, *Council Directive 95/46 of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data:*, [1995], O.J.L. 281/31 at 1 [Hereinafter *Personal Data Directive*]

[244] The CCBE (Council of the Bars and Law Societies of the European Community) has enacted a Code of conduct for Lawyers in the European Community. In which it is stated (2.3.1): " Without the certainty

$80,000 was offered for any laptop belonging to any Fortune 100 executive.[245] In a case relayed to the CRISIS committee, a laptop belonging to an executive of a large multinational company was seized at the customs. Later on the owner of the laptop found out that the opposite party had accessed all the information in his laptop.[246] As the examples above show cryptography is only one, but on the other hand a very useful method to prevent unauthorized access and alteration of data.

Situations in which liability might be an issue

Revocation of keys

Without doubt cryptographic keys will get lost in one or another way, by accidents, negligence and, for example, fraud. A system for revocation of keys therefore needs to be established. If for example a vendor of cryptographic products has sold a cryptography product to a company and an employee of that company one day loses the key that he has used to encrypt the customer register for the company, can the vendor of the cryptographic product then be held liable for not having clearly stated that lost keys were unrecoverable? Does the vendor have a duty to inform? Another example where access to keys might be necessary is for beneficiaries to estates of deceased.[247] A major issue is whether public authorities can revoke keys that have been used in criminal activities or prohibit individuals from encrypting? Does the right to free speech supersede public order considerations?[248]

---

of confidentiality there cannot be trust. Confidentiality is therefore a primary and fundamental right and duty of a lawyer." This duty to observe confidentiality also stretches to unauthorized access to confidential information.

[245] D. Costa, "Not-So-Soft-Security," (1995) August, *Mobile Office*, at 75

[246] Crisis *supra* note 67 at 471

[247] In these cases there might be a sensitive balance for courts to order for example a key recovery agent to hand over the keys. Which rights for example do the beneficiaries of the estate have to the deceased's private mail and signature keys? It will difficult whit this type of situations where there is no one to ask? Did the deceased intend to take confidential information with him to the grave?

[248] An interesting case is the Bernstein case. *Bernstein v. USDOJ* available online at http://www.steptoe.com/webdocs.nsf/files/bernstein/$file/bernstein.html (date accessed: 21 August 2000)

Risk of compromised keys

Fear of liability issues might restrain people from using cryptographic systems because of the risk involved with compromised keys.[249] One solution for users as well as for vendors seems to be to use cryptographic systems endorsed by the government. If a business entity uses a government-endorsed cryptographic system it will be hard to argue that the private entity has not exercised due diligence, since it is hard to argue that a cryptographic system endorsed by the government does not comply with reasonable standards. If liability issues are unclear individuals as well as business will hesitate to start using new and perhaps better-suited cryptographic systems. There will be a lock-in effect that hinders the development and use of secure new systems.

Liability for governments which holds keys in escrow

An interesting and fundamental question is the liability for a government which holds keys in escrow. Will governments be prepared to assume liability if keys get compromised when in their possession? There is no link in the OECD Cryptography Guidelines between liability and lawful access. Liability could potentially open up the flood gates to lawsuits that would involve substantial amounts of money. Without reading the explanatory text simultaneously one does not understand much of the principle of liability in the Cryptography Policy Guidelines. The principle mentions that liability can be established either by contract or legislation. This does not make much sense until one reads the explanatory text, which says that potentially liable entities includes governments. The Cryptography Policy Guidelines hence aim at both key management systems and key access systems.

The Cryptography Policy Guidelines moreover raise a difficult problem that has to be split up, since liability arising from key access systems on the one hand and key management systems on the other raises different problems. Liabilities arising out

[249] The Utah Digital Signature Act (1995) has not been the veritable success that Utah claimed it was when it was presented, mainly because of liability reasons. Certification authorities may under the Utah Digital Signature Act, issue certificates. According to the Act " the private key corresponding to the public key listed in the certificate is a legally valid signature of the subscriber". A certificate certifies furthermore that " an unauthorized person does not have access to a private key. See Utah Digital Signature Act §§46-3-302(1) and 46-3-401(1) The potential risk of being sued for liability has held back the use of cryptography.

of a key access systems such as the Clipper chip initiative will be rather complex as they will involve international as well as national legislation. National legislation will involve federal and provincial levels in many countries, which will make key schemes quite complicated. A governmental database, holding for example private keys, will presumably be liable if secret keys are compromised.[250] It is, however, up to governments to limit their liability by legislation. At first sight it does not seem to be particularly complicated but it certainly becomes complicated when you move up to an international level. If for example the U.S. Government is holding the secret keys belonging to a citizen or corporation in another country, then the question of liability has to be solved through public international law. The easiest way to solve this kind of problem would be through multilateral and bilateral agreements. When it comes to key management systems,[251] a contract will exist between the keyholder and the trusted third party. I do not perceive as much a problem existing here as when a government is holding the keys. The limits of liability have to be defined through contract. If a trusted third party or certification authority is going to accept liability, they will require a fee, which is not going to be low. Trusted third parties or certification authorities will probably have to insure themselves. The cost of insurance will be passed on to the customers, i.e.the keyholders.

Liability for misused personal information in databases at certification authorities

According to Article 23 in the EC Personal Data directive, a person who has suffered damages as a result of an unlawful processing operation or any act incompatible with national provisions adopted pursuant to the directive, has the right to receive compensation from the controller. The controller can only exculpate himself by proving that he is not responsible for the events that gave rise to the damage. As the directive suggests it is up to the Member states to set the range of liability for unauthorized access. The directive only states that the claimant should be entitled to compensation and not damages, which is wider. CAs will undoubtedly fall into the category that will

[250] This was the case in Son of Clipper (Clipper II was another name) or Software key escrow as the U.S. Government named it. In Clipper II the key escrow system was intended to hold access to the private keys through a backdoor into the algorithm that controlled the encryption.
[251] The term key management system is used as a term for a voluntary system.

be liable to pay compensation because of an illegal processing action, since they will posses personal information.

6.4.8 INTERNATIONAL CO-OPERATION

GOVERNMENTS SHOULD CO-OPERATE TO CO-ORDINATE CRYPTOGRAPHY POLICIES. AS PART OF THIS EFFORT, GOVERNMENTS SHOULD REMOVE, OR AVOID CREATING IN THE NAME OF CRYPTOGRAPHY POLICY, UNJUSTIFIED OBSTACLES TO TRADE.

In order to promote the broad international acceptance of cryptography and enable the full potential of the national and global information and communications networks, cryptography policies adopted by a country should be co-ordinated as much as possible with similar policies of other countries. To that end, the Guidelines should be used for national policy formulation.

If developed, national key management systems must, where appropriate, allow for international use of cryptography.

Lawful access across national borders may be achieved through bilateral and multilateral co-operation and agreement.

No government should impede the free flow of encrypted data passing through its jurisdiction merely on the basis of cryptography policy.

In order to promote international trade, governments should avoid developing cryptography policies and practices which create unjustified obstacles to global electronic commerce. Governments should avoid creating unjustified obstacles to international availability of cryptographic methods.

Co-operation to co-ordinate

This principle is definitely one of the most important of all the principles, since divergent national cryptography policies will hinder the development of secure global telecommunications, which is vital for the economy. The only way to create a truly secure borderless and seamless international information and communication network is through international co-operation. The OECD Cryptography Policy Guidelines represents the best initiative so far to achieve international co-ordination.

Internationalization

Business has become increasingly international over the last decade and multinational corporations have offices and management in several countries. We are also experiencing a wave of consolidation and the number of mergers and acquisitions have reached new record highs. The number and complexity of international trade

agreements have, furthermore grown considerably the last two decades.[252] These developments have created a genuine need for international communications. The shift in international trade is towards greater openness. Restrictive national cryptographic policies represent an obstacle to this shift towards greater openness.

The principle

It should be noted that the principle speaks about international co-operation to co-ordinate rather than harmonize disparate national cryptographic policies.

One of the purposes behind the OECD Cryptography Guidelines is to operate as a framework for national cryptographic policies. To what extent the OECD Cryptography Policy Guidelines will be useful for this purpose remains to be seen. Several countries refer to them in national cryptographic policies, but the essential question on how use and import/export of cryptography should be regulated has been left to further negotiation.[253]

What is the difference between co-ordination and harmonization? Harmonization represents an additional step that brings policies in line with each other. Co-ordination is merely a way of removing sharp edges. Harmonization is usually achieved within an organization via some kind of enforcement mechanism. Since the OECD is only an interest organization the OECD Council has stopped at international co-ordination rather than international harmonization which would have been preferable. Hopefully, the OECD Cryptography Guidelines will serve as a medium and in the end harmonize disparate national policies anyhow. No country has anything to gain from not co-operating if they want to continue to develop economically. The present difficulties with interoperability and mobility will also be worse when cryptographic features are added to telecommunication systems. The chances of implementing a trustworthy and safe encryption scheme will moreover be greater if

---

[252] The EC has become the EU and a monetary union is in progress, the WTO has been negotiated as well as other international trade agreements such as the NAFTA.

[253] See the OECD, Group of Experts on Information Security and Privacy, Directorate for Science, Technology and industry, Committee for information, Computer and Communication Policy *Review of the 1992 Guidelines for the security of information systems*, DSTI/ICCP/REG (97) 2/Final, 19 March 1998 at 12. The committee which reviewed the 1992 Guidelines suggested that a work program should be developed to take issues related to Electronic Commerce forward. See also *A Cryptography Policy for*

steps are taken at an early stage, since security solutions implemented at a late stage often achieve far less satisfactory results.

Sharing Common Ground – International aspects contra national interests

Even though most states seems to agree that international consensus is essential, such consensus will be hard to achieve for cryptographic policies for a number of reasons. National sovereignty and national security, economic interests and international law enforcement are some of the issues that will be difficult to negotiate.[254] All countries want to maintain their international independence and sovereignty. Compromises that involve foreign custody of encryption keys in key escrow systems or key recovery systems will result in loss of sovereignty. Very few countries will therefore be willing to accept such a system since countries have varying obligations to respect, for example, privacy and public order. In the United States individual citizens are more concerned with government intrusion than in Europe. In Europe, on the other hand, people in general are more concerned with data gathering (data mining) from private subjects.

National security goes to the very root of the national state and represents a stumbling block on the way to reaching international co-operation for a number of reasons. Agreements regarding national security interests, for example on information sharing, are very seldom public and it is quite understandable that countries have different interests to protect.[255] Economic interests will also vary between countries. Countries have different interests to protect, for example national cryptographic industries, or national businesses against foreign espionage. States therefore have an

---

Electronic Commerce- Building Canada's Information Economy and Society, (Ottawa: Industry Canada, 1998), which refers to the OECD Cryptography Policy Guidelines specifically.

[254] The competence of Member States regarding national security and law enforcement is fully recognized in the EC Treaty and the Treaty on the European Union. National restrictions that are put in place have, however, to be justifiable under Community law. For cryptography the provisions regarding free circulation and the Data Protection Directive are of special interest. See *Towards A European Framework for Digital Signatures and Encryption, supra* note *192* at 20

[255] Echelon, the intelligence gathering system led by the NSA has caused public debate within the EU. According to an article called "Generande spioneri i vänkrets" (Bothering spying in a circle of friends (my translation)) Ylva Nilsson, Svenska Dagbladet (31 March 2000) at 1. Echelon is capable of intercepting billions of telephone calls, facsimile transmission and e-mails. The EU parliament has now requested a public debate regarding the Echelon.

interest to control the use of cryptographic products.[256] It is also difficult to reach international agreements because of different views on law enforcement.
Despite these divergent views there are some areas where many countries share a common interest. Law enforcement is one area where countries also, despite different attitudes to certain crimes, also share a common ground. Genocide, terrorism and drug dealing are crimes that are condemned in most countries.[257] These crimes are, moreover, often international in character, which makes it necessary for more than one country to combat them.[258] An area in which countries will be forced to co-operate is international telecommunications. The largest issue that will force countries to co-operate and co-ordinate despite divergent national cryptographic policies is the economic growth in the new economy and especially the potential of electronic commerce.

International Agreements

National cryptographic policies have to comply with other international agreements and undertakings such as the Wassenaar Arrangement. Although it is mentioned in the principle that governments should remove, or avoid creating, in the name of cryptography policy, unjustified obstacles to trade, existing national regulations that implement international agreements cannot be seen as unjustified.[259] National cryptographic policies moreover have to be compatible with international trade agreements. These trade agreements will probably have a more profound impact on

---

[256] National security agency involvement in espionage and also counterintelligence has become more common since the cold war ended. There has been a shift towards economic interests rather than political. It has been suggested that the NSA led Echelon is used to intercept sensitive economic electronic information as well. According to Barbara McNamara, Deputy Director of the NSA, the NSA now wants to balance security with privacy while ensuring threat against foreign intelligence when necessary. "NSA now wants a global information infrastructure so that people using encryption will know who is who" See D. McGullagh"NSA balancing Security, Privacy", 1 April 2000, online: http://www.wired.com/news/politics/0,1283,35331,00.html (date accessed: 1 April 2000)

[257] International consensus regarding these crimes has been achieved as a result of international negotiations.

[258] See for example P. Williams, *Transnational Criminal Organizations and International Security,"* Survical, Volume 36 (1), spring 1994 ff 96 and regarding computer crimes *United Nations Manual on the Prevention and Control of Computer- Related Crime,*online: http://www.ifs.unvie.ac.at/~pr2gq1/rev4344.html (date accessed: 1 November 1997)

[259] See *Orlowski, supra* note 165 at 278

national cryptographic policies since these agreements are binding, while the OECD Cryptography Policy Guidelines are not.

Co-ordinating harmonization of Control Regimes Regarding Cryptography

International co-operation and co-ordination will be necessary for all countries controlling cryptography. Efforts will be required from different directions. Use of cryptographic products might for example be illusory if cryptographic products are not allowed to be connected to the public telephone net. Certain licensing regimes might also be imposed that make it very difficult to import cryptographic products. Imposed national standards that are non- compliant with international standards might moreover restrict the use of cryptography. Some states might try to restrict the import and use of cryptography through such trade agreements. Such actions will however interfere with competition laws as well as the principle of free choice of cryptographic methods, as well as the principle of co-operation, which refers to unjustified obstacles to trade.[260] The mentioned barriers to import and use that countries might impose will also be a violation of the spirit of the explanatory text, which states that governments should avoid creating unjustified obstacles to international availability of cryptographic products.[261]

National cryptographic polices as an obstacle to trade

The principle states that national governments should take active steps to remove existing obstacles that a national cryptographic policy might impose. Governments should, furthermore, refrain from creating new unjustified obstacles to trade in the name

[260] See also Crisis *supra* note *67* at 436.

[261] Several of these measures can be circumvented fairly easily. A satellite telephone do, for example, link up directly to a satellite without going through the telephone network. Nothing prevents a user from encrypting a message twice. (so called superencryption) Encryption might be done once with an encryption program that does not comply with the standard and then once again with an approved encryption program. The only possibility to detect superencryption is to analyze the text itself. This might, however, mean that all encrypted messages have to be analyzed, not only the encrypted messages that are standing out. Use of superencrytion would therefore put additional strain on analyzing capabilities and force intelligence agencies to focus on certain sources from the beginning instead of scanning a greater number of messages.

of cryptographic policy.[262] Even though the principle suggests that national governments should remove present obstacles, there is no reference to whether such obstacles are justified or not. What are unjustified obstacles to trade?[263] Some sort of exception was necessary when the Cryptography Guidelines were drafted because agreements, such as the earlier mentioned Wassenaar arrangement, had to be provided for. It is notable that the Guideline uses the term "unjustified" and not unjustifiable.[264] The interpretation of unjustified is left to the member states thereby making the guideline weak. In this respect unjustified undoubtedly refers to law enforcement access and national security interests.

What does it then mean that governments should refrain from creating new unjustified obstacles to trade? It is obvious that the term "unjustified" is measured against the value of free trade, but it is less clear what level of restriction qualifies as unjustifiable. According to Stewart Baker, the term "unjustified"is borrowed from international trade law, where the term has been defined by usage.[265] Baker suggests that it should be interpreted in such a way that no government should use cryptographic policy to discriminate against foreign products. This interpretation seems reasonable.The question is, however, whether national policies might infringe other international trade agreements such as the WTO or the NAFTA agreements.[266]

---

[262] One market where national cryptographic policies create obstacles to trade is, of course, the cryptographic market. This market is getting larger and larger and one of the most influential lobby groups for unrestricted use and export of cryptographic products is the cryptographic software industry.

[263] According to S. Baker, *supra* note 162 (Decoding the OECD's Guidelines for Cryptography, http://www.steptoe.com/comment.htm (date accessed: 2 November 1997) OECD by choosing "unjustified" instead of "unjustifiable" called upon member states to proffer understandable justifications for their policies on cryptography. He is of the belief that the text applies specifically to unjustified obstacles to international availability of cryptography. This, he means, opens up the door to requests that nations justify their export control regimes as well as their import and domestic policies. If one reads the text in the Guideline carefully the word "international" is not mentioned. It is only in the explanatory text "international" is mentioned. The principle has preference over the explanatory text. One might consider whether the present U.S. export cryptography regulations in itself creates an obstacle to trade. United States software companies controls more than 80 % of the market and that has, of course, an impact on trade.

[264] *Ibid,* S. Baker, *supra* note 162 thinks the term have been adopted from the WTO agreement. In my opinion it is questionable whether one can interpret "unjustified" in the light of the WTO agreement.

[265] See *Orlowski supra* note 192 at 278 see also Decoding the OECD Cryptography Guidelines *supra* note 162 at 8.

[266] In the US Congress, critics have seized on the issues regarding China's new regulations providing that Companies have to register encryption programs and divulge information of the main encryption capabilities as well as send examples for inspection. The Congress will during the spring of 2000 vote whether to grant China permanent trade relations. The vote is seen as a test and prerequisite to China's

It is stated in the explanatory text that governments should refrain from impeding the free flow of encrypted data passing through their jurisdictions.[267] Access to such data has to be gained through bilateral or multilateral agreements. This seems to be a direct reference to the European Union Directive about transborder data flows, which states that no government should impede the free flow of encrypted data passing through its jurisdiction. States cannot therefore not justify restrictions in the free flow of data by reference in their cryptography principles.[268] One may ask in fact whether it is possible to control all communication to, from and through a country. No government, even with the most sophisticated intelligence capability, will probably be able to monitor and stop all encrypted information floating into the country. Information as such is not transferred as sentences but as ones and zeros in a binary system. Traffic analysis probably has to be specified against a specific target because of the sheer volume of data traffic. The statement therefore seems somewhat far-reaching. Some countries have however restricted access to the Internet as a matter of social control over their citizens.[269] This is, however, a rather extreme method. It is furthermore difficult to enforce such restrictive measures. The OECD Cryptography Policy Guidelines are clearly a compromise between countries favoring key access systems and countries favoring a more market-based approach.

The explanatory text also mentions that if national key management systems[270] are developed such systems must allow for international use of cryptography.[271] The USA certainly does not trust other countries since they have been lobbying for a key management system with keys stored in the USA. Even though the explanatory text

---

WTO accession. See J. Kynge, "Encryption rules to hit Chinese software trade", *Financial Times* 28 January 2000 at 6.

[267] This approach is consistent with the approach taken by the International Telecommunication Union.

[268] According to S. Baker, the principle is borrowed from a strong ITU rule against actions that impede the free flow of international communication. *Decoding supra* note 162 at 5

[269] Other examples are Saudi-Arabia and North Korea. China has recently enacted new regulations that will force companies to register with the State Encryption Management Commission if the company is distributing, selling or using encryption technology. Companies will moreover later be required to divulge information on the main encryption capabilities of the programs or products and send examples for "inspection." See further J. Kynge *Supra* note 266, "Encryption rules to hit Chinese software trade", *Financial Times* 28 January 2000 at 6

[270] The term Key management system is used in a broad sense to include storage and archiving of cryptographic keys which essentially are key escrow or key recovery.

[271] One might wonder why "where appropriate" has been put there since it leaves it up to the member states to decide whether it is appropriate or not.

states that national key management systems must allow for international use of cryptography such a system will be hard to establish in practice.

CONCLUSION

The OECD Cryptography Policy Guidelines have been criticized as being weak and contradictory. They are contradictory in many aspects, but as in the case of all international agreements they are based on compromises between different interests. A choice has to be made in the end after the interests at stake have been balanced. Basically there are policies which could be followed: Either regulate and restrict use of encryption or not regulate. In my view four main arguments speak for unrestricted use and export of cryptography and for leaving it up to the industry itself to develop a standard:

International aspects

The world we are living in is becoming more and more global. In the beginning of the century trains, cars and ships were bringing the world together. Today it is the Internet that brings the world and people together. The Internet offers great opportunities in communication and trade. To ensure trade on the Internet the networks used need to be secure. Encryption is one of the best, but not the only way, to achieve security. Any encryption standard that is developed has to be accepted globally in order to be a successful international standard. Access to government held keys has furthermore to be negotiated with other countries if a government key access system is adopted. These negotiations are going to be difficult, since the question of governmental access is so closely connected with sovereignty and national security. Earlier international conventions in the area of cooperation regarding law enforcement have taken a long time to negotiate. These negotiations that probably will go even further will take even longer to negotiate.

If the development is left to the market, standards will probably be developed faster than if governments are to negotiate about such sensitive issues as sovereignty, national security and competition. Any encryption standard that is developed has furthermore to be flexible and must be able to follow technological development for a considerable period of time and scaleable. Information might need to be protected for periods up to 50 years. It will be very difficult to negotiate such a standard.

Liability

This is a very interesting issue and unsolved problems regarding liability issues exist on several levels, international, national and, to some extent, provincial. The most challenging problem to solve is without doubt liability from an international perspective, especially if a government key access system is adopted. If will be difficult to come to an international agreement as to what extent a government should be liable if keys are, for example, compromised. If government agencies hold private keys in escrow this might open up the floodgates to unlimited liability for governments. Another interesting issue concerns liability in key management systems. How should liability be allocated in such a system? In the end the cost will be transferred to the user and the cost for using a system is very important for the user. It is therefore essential that the costs are kept reasonably low. Large corporations will always have the possibility of insuring themselves. To obtain coverage for an individual will be much more difficult. In the end it will be the users that will have to pay for the insurance or take the risks. Risks will be better allocated within a free and undistorted market.

Law and economic arguments

If the responsibility for developing a standard rests on the industry then the industry itself will have to pay for maintenance and improvement. If a government key access system is adopted the government will have to pay for the maintenance of the system, not to mention the cost for safeguarding the keys held in escrow and the potential liability. In a free market system there is self-regulation of cost versus need. The consumer gets what he needs and is paying for. In a free market different levels of encryption probably will develop as well as different individual solutions regarding insurance. In a market system liability will be distributed amongst the users and certification authorities based on who can control the risk of keys being compromised. In a government key access system the government will have to bear the brunt of the cost for the system.

Legal control

The most important thing to ensure, as emphasized in the Cryptography Policy Guidelines, is user trust. If the user does not trust the cryptographic system completely it will not be used and will rather hinder the development of security. One of the problems with government control lies in trust in the government. Trust is a more fundamental question than law enforcement access. The true underlying reasons for restricting access to strong encryption seems, moreover, to be fear of loss of intelligence capability in for example the international Echelon[272] system rather than difficulties faced by law enforcement agencies in combating crimes. Law enforcement agencies have access and they should continue to have access. Access should, however, be under strict judicial control. There seems, at least in the USA, to be a fear that governments might circumvent established judicial controls of access over private and confidential information.

Terrorism and access to cryptography

It should be remembered that much terrorism is state supported. These terrorists will have access to encryption anyhow, supplied by the country that supports them. A final argument is that there is no monopoly on encryption even though it will be easier to introduce a standard if it is included as a part of a operating system. Several encryption systems, such as Pretty Good Privacy, are already widespread. Furthermore are product development regarding cryptography being established in countries where legal control is less far reaching. There is therefore reason to believe that the battle for regulating encryption will be lost in the long run anyhow.

Convergence

It seems that we presently not moving towards convergence. The OECD Cryptography Policy Guidelines will, however, serve as a useful starting point for further negotiations. The OECD represents a valuable forum for international co-operation and co-ordination and the work continues. The OECD ministerial conference on electronic

[272] The earlier mentioned intelligence system that is operated by USA and UK.

commerce held in Ottawa, October 7-9, 1998, focused on the legal framework, institutional arrangements and technical infrastructure needed to support an international marketplace for electronic commerce.[273] More conferences were held during 1999 and will continue through 2000. Among the areas covered during the Ottawa conference were the protection of personal information and privacy, the rights and obligations of consumers and authentication for electronic commerce.[274] These issues will remain important as we move into a more digital and global economy. It is regrettable, but understandable, that the OECD negotiations regarding the Cryptography Policy Guidelines did not reach further. They will, however, be an important step in the development and revolution of cryptography.

[273] "General presentation", online: http://www.stategis.ic.gc.ca/html (date accessed:26 October 1998).

[274] The private sector is important to reach a broad consensus for policy questions. Several organizations such as BIAC (the Business and Industry Advisory Council) the ICC (International Chamber of Commerce), the ILPF (Internet Law and Policy Forum), WITSA (the World IT and Service Alliance) and the GIIC (Global Information Infrastructure Commission) have therefore been invited.

BIBLIOGRAPHY

GOVERNMENT DOCUMENTS

OECD

The Convention for Economic Co-operation and Development (Paris: 11 September 1960)

Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data, [C(80)58(Final)] (Paris: 23 September 1980)

The Declaration on Transborder Flows, [Annex to C(85)139] (Paris: 11 April 1985)

Recommendation of the Council concerning Guidelines for the Security of Information Systems, [C92)188/Final] (Paris: 26-27 November 1992)

General Secretariat, Liaison and Co-Ordination Unit, Committee for Information, Computer and Communication Policy, OECD Emerging Market Economy Forum, *Report On The Workshop On Cryptography Policy*, SG/EMEF/ICCP (98)1, (Paris: December 1997)

General Secretariat, *Implementing the OECD "Privacy Guidelines" in the Electronic Environment: Focus on the Internet* DSTI/ICCP/REG(97)6/FINAL

Group of Experts on Information Security and Privacy, Directorate for Science, Technology and industry, Committee for information, Computer and Communication Policy, *Review of the 1992 Guidelines for the security of information systems"*, DSTI/ICCP/REG (97) 2/Final, (Paris:19 March 1998)

Canada

A Cryptography Policy for Electronic Commerce- Building Canada's Information Economy and Society (Ottawa: Industry Canada, 1998)

USA

Administration of Export Controls on Encryption Products, The White House, Office of the Press Secretary, Executive Order, (Washington: 15 November 1996)

Codes, Keys and Conflicts: Issues in US Crypto Policy, Report of a Special Panel of the US Public Policy Committee, June 1994, The White House, Office of the Vice President, Statement of the Vice President, (Washington: 1 Oct 1996)

Computer Science and Technology, Computer Security and the Data Encryption Standard, Proceedings of the Conference on Computer Security and the Data Encryption Standard, Gaiterburg, MD, Special Bureau of Standards, Special Publication 500-27(Washington D.C, U.S Government Printing Office, (1978) (CNBS SP500-27)

Digital Signature Standard, Office of Technology Assessment Information Security And Privacy in Network Environments, OTC-TCT-606, (US Government Printing Office, Washington D.C., 1994)

Other

The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies (Wassenaar 11 - 12 July 1996)

Council of Europe, Committee of Ministers, *Recommendation [R(95)13] concerning problems of criminal procedural law connected with information technology*, (11 September 1995)

LEGISLATION

EC/EU

EU, *Council Directive 95/46 of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data an on the Free Movement of such Data:*, [1995] O.J.L. 281/31

EC, *Council Regulation of 31 August, 1992 establishing The Treaty on the European Union*, [1992] O.J.L. 24/1

EC, *Council Regulation 3381/94 of 19 December 1994 setting up a Community regime for the control of export of dual-use goods*, [1994] O.J.L 82/1

EU, *Council Decision 94/942/CFSP of 19 December 1994 on the joint action concerning the control and use of dual-use goods*, [1994], O.J.L 90/1

EU, *Council Directive 1999/93 of 13 December 1999 on a Community framework for electronic signatures* [2000] O.J.L 13/12

Other

UN

ICAO, *The Convention for the Unification of Certain Rules Relating to International Carriage by Air* signed at Warsaw 12 October 1929. Amended at the Hague, 28 September 1955, reprinted in: L.B. Goldhirsch, *The Warsaw Convention annotated* (Dordrecht, The Netherlands: Kluwer, 1988) 185 ff.

Universal Declaration of Human Rights, GA Res., 217 (III), UN GAOR, 2d Sess., Supp. No. 13, UN Doc. A/810 (1948) 71

International Covenant on Economic, Social and Cultural Rights GA Res 2200 A (XXI) 1966, reprinted in: Council of Europe, *Human Rights in International Law, Basic Texts (Strasbourg, France: Council of Europe Press, 1992).*

France

Loi no 90-1170, du 29 decembre 1990 (Art. 17 amending Article 28). (Telecommunication Act No 96-059)

Telecommunications Act No 96-659.

Russia

Edict No. 334, of the Russian Federation on measures to Observe the Law in Development, Production, Sale and Use of Encrypting Information (3 April 1995) (Replaced by Edict of 3 April 1995)

Sweden

The Swedish Computer Act "Datalagen" (SFS 1973:289)

The Personal Data Act "Personuppgiftslag" (SFS 1998:204)

USA

Utah Digital Signature Act 1995

Computer Security Act, (Public Law 100-235)

BOOKS

Ahlström, C, *The Status of Multilateral Export Control Regimes-An Examination of Legal and Non-Legal Agreements in International Co-operation* (Uppsala, Sweden: Iustus, 1999)

Allen, A.L, *Uneasy Access:Privacy for Women in a Free Society*, (Lanham, MD: Rowman and Littlefield, 1995)

Baker, R.H, *Network security: how to plan for it and achieve it*, 1 ed. (New York: McGraw-Hill, 1995)

Baker, s.A & Hurst, P.R, *The Limits of Trust Cryptography, Governments and Electronic Commerce*, (Cambridge, MA: Kluwer, 1998)

Barett, N, *Digital Crime: Policing the Cybernation* (London: Kogan, 1997)

Bennett, C, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States* (Ithaca: Cornell University Press, 1992)

Brassard, G, *Modern Cryptology- A tutorial-Lecture Notes In Computer Science* (New York: Springer – Verlag, 1988)

Burnham, D, *The Rise of the Computer State*, (New York: Random House, 1983)

Campen, A.D, *The First Information War* (New Jersey: AFCEA International Press, 1992)

Cargill, C.D, *Information, Technology & Standardization* (Bedford, Massachusetts: Digital Press, 1989)

Carlén-Wendels. T, *Nätjuridik- Lag och Rätt på Internet* (Stockholm: Nordstedts Juridik, 1998)

Ceiller, R, *La Cryptographie*, Que sais-je?, vol 116 (Paris: Presses Universitaries de France, 1945)

Cohen, F, *Protection and Security on the Information Highway* (New York: John Wilsey & Sons, 1995)

Dam, K.W, *Cryptography's Role in Securing the Information Society*, National Research Council, Computer and Telecommunications Board (Washington DC: National Academy of Sciences, National Academy Press, 1996)

Danby, H, *The Misnah* (Oxford: Oxford University Press, 1933)

Diffie, W and Landau, S, *Privacy on the Line- The Politics of Wiretapping and Encryption* (Cambridge, MA: MIT Press, 1998)

Dworkin, R, *Life's Dominion, An argument about Abortion, Euthanasia, and Individual freedom* (New York: Alfred A. Knopf, 1993)

Flaherty, D.H, *Protecting Privacy in the Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada and the United States* (Richmond: University of North Carolina Press, 1989)

Friedman, L, *A history of American Law* (New York: Simon and Schuster, 1973)

Garlinski, J, *Intercept: The Engima War* (London: J.M. Dent and Sons, 1979)

Godin, S, *Presenting Digital Cash*, 1 ed. (Indianapolis: Sams.net Publishing, 1995)

Grengrass, P, *Spy Catcher* (Victoria: Heineman Publishers Australia, 1987)

Hobbes, T, *Leviathan* (1651), Part I and II, (Indianapolis: Bobbs-Merrill, 1951)

Hyatt, G, *Stump the Cipher Punks*, in Networks 2000 Internet, Information Superhighway, Multimedia Networks and Beyond, 1st ed. (New York: Miller Freeman, 1994)

Johnston, D, Cyberlaw: *What you need to do business online*, 1st ed, (Toronto: Stoddart, 1997)

Johnston, D, *Getting Canada online: understanding the information highway*, 1 ed. (Toronto: Stoddart , 1995)

Kahn, D, *The Codebreakers, The story of secret writing* (New York: Macmillan, 1967)

Kahn, D,, *Kahn on Codes* (New York: Macmillan, 1983)

Luce, D, and Raiffa, H, *Games and Decisions* (New York: John Wiley & Sons, 1957)

S. Landau et al., *Codes, keys and Conflicts Issues in US Crypto Policy* (Washington D.C: Association for Computing Machinery, 1994)

Lyon. D and Zureik, E, eds., *Computers, Surveillance, and Privacy* (Minneapolis: University of Minnesota Press, 1996).

Menezes, A,Von Oorchot, P and Vanstone, S, *Handbook of Applied Cryptography* (Florida: CRC Press, 1996)

Nugter, A.C.M, *Transborder Flow of Personal Data within the EC: A Comparative Analysis of the Private Statutes of the Federal Republic of Germany, France, the United Kingdom and the Netherlands.* (Antwerpen: Kluwer, 1990).

Reagan, P.M, *Legislating Privacy: Technology, Social Values, and Public Policy* (University of North Carolina Press, 1995)

Reinhold, A.G., *Internet Privacy and Security*, in John R. Levine & Carol Baroudi: *Internet Secrets*, 1 ed. (Foster City, CA: IDG Books Worldwide,1995)

Rosseau, J.J, *The Social Contract* (1762) (Harmondworths, Penguin Books, 1968)

Schneier, B, *Applied Cryptography; protocols, algorithms, and source code in C*, 2nd Ed (New York: John Wiley & Sons, 1996)

Schoeman, F.D ed., *Philosophical Dimensions of Privacy: An Anthology* (Cambridge, Massachusetts: Cambridge University Press, 1984)

Schotter, A, *The Economic Theory of Social Institutions* (Cambridge: Cambridge University Press, 1981)

Skogh, G, *Den osynlige handen och lagens långa arm*, in *Ekonomi under debatt*, Göran Skogh ed, (Malmö: Liber, 1983)

Smith, J.F, *Managing Privacy: Information Technology and Corporate America* (Chapel Hill. University of North Carolina Press, 1994)

Smith, R.E, *How to protect Privacy- What's Left of It* (New York: Anchor Press, 1979)

Stallings, W, *Make it real* in Networks 2000 Internet, Information Superhighway, Multimedia Networks and Beyond, 1st ed. (New York. Miller Freeman, 1994)

Stallings, W, *Practical cryptography for data and Internet networks*, 1 ed. (Los Alamitos: IEEE Computer Society Press)

Torvund, O, *Elektronisk handel via Internett, Elektronisk handel –rättsliga aspekter, Nordisk årsbok i Rättsinformatik 1997* (Stockholm: Nordstedts Juridik, 1997)

Wallace, J.D, *Sex, laws and cyberspace: freedom and regulation on the frontiers of the online revolution* (New York: Henry Holt and Company, 1996)

Wayner, P, *Digital Copyright Protection* (New York: AP Professional, 1997)

Wayner, P, *Disappearing Cryptography* (London: AP Professional, 1996)

Wendels, t.C, *Nätjuridik-Lag och Rätt på Internet*, 2 ed. (Stockholm: Norstedts Juridik, 1998)

Westin, A.F, *Privacy and Freedom* (New York: Athenum, 1967)

Voltaire, (Arouet, F.M) *Dictionnaire Philosophique* (1769)

Wright, P, *Spycatcher* (New York: Viking Penguin, 1987)

Yardley, H.O, *The American Black Chamber* (Indianapolis: Bobbs Merill, 1993)

ENCYCLOPEDIAS AND DICTIONARIES

The American Heritage Dictionary of the Language, 3rd Ed., (Boston: Houghton Mifflin, 1992)

The Hutchinson Encyclopedia, 8th Ed., (London: George Philip & Sons., 1988)

ARTICLES, ADDRESSES AND PAPERS

Archer, "Beyond the Firewall" (August 1997, issue 7)), Internet Business Magazine at 38

S. A. Baker "Don't worry be happy-Why Clipper is good for you" (2.06) June 1994, Wired Magazine

C. Benett et al., "Quantum Cryptography" (1992), vol 267 (4) October, Scientific American

U. Björkstén, "Autopilot invaggar pilot i falsk säkerhet", *Svenska Dagbladet* (5 December 1999) at 11

"Canadians are accustomed to immigrants" *The Economist* (15 November, 1997)

B. Cipra, "Electronic Time-Stamping: The Notary Public Goes Digital" (1993) 261 Science at 162

D. Costa, *Not-So-Soft-Security* (August 1995), Mobile Office at 75

D. Denning & Branstad, "A Taxonomy for key Escrowed systems" (March 1996), 39 Coom ACM 36

D. Denning; "Encryption and Evolving Technologies as Tools of Organised Crime and Terrorism", The National Strategy Information Centre's U.S. Working Group on Organised Crime (WGOC).

C.A. Devours, "Unicity points in cryptanalysis" (1977), vol. 1, Cryptolgia

P.E.-Dewitt "Terror on the Internet", *Time* (12 December 1994) at 73

W. Diffie and M.E. Hellman, "Exhaustive Cryptoanalysis of the NBS Data Encryption Standard", June 1977, v.10, n. 6, Computers at 74

Electronic Commerce: Analysis of a New Business Paradigm (August 1997) Internet Business 7, JCP Computer Services at 36

C.L Evans,. "U.S. Export Control of Encryption Software: Efforts to Protect National Security Threaten the U.S. Software Industry's Ability to Compete in Foreign Markets" (1995) ,19 North Carolina Journal: International Law and Commerce Regulation ,

J. Flinn, *San Francisco Examiner* (1 November 1992) at 3

"Fraudulent Fax Gets Forger Freed", *San Francisco Chronicle* (18 December 1991) at 3

M. A. Froomkin, "The Metaphor Is The Key: Cryptography, The Clipper Chip And The Constitution" (1995), 143, University of Pennsylvania Law Review at 753

S. Handa and M. Branchaud, "Re-evaluating Proposals for a Public Key Infrastructure." (1996) 29 Law/Technologhy J. at 1

G. Johnson, "The spies, Code and how it broke", *New York Times*, Week in review (16 July 1995) at 4

P. Kinnucan, (Tuchman and Meyer) "Data Encryption Gurus" (1994) vol. II, no. 4:, Cryptologia at 371

B. Kuner. "Legal Aspects of Encryption in the Internet" (1996), April, International Business Lawyer at 6

J. Kynge, "Encryption rules to hit Chinese software trade", *Financial Times*, 28 January 2000

G. Leeming "A New Business Paradigm" (August 1997, issue 7) Internet Business Magazine at 37

A. Marshall, Encryption (August 1997, issue 7) Internet Business Magazine at 44

Neuman, "Computer-Related Risks", *San Francisco Examiner*, 1 November 1992

Y. Nilsson, "Generande spoioneri i vnkrets", *Svenska Dagbladet* 31 March 2000 at 1

P. Odebrant "Bankerna förlorar 63 kr i sekunden", 1999, no 4, Aktuell Säkerhet 24

S. Orlowski, "Cryptography Policy-The OECD Cryptography Guidelines" (1997) 13:4 Computer Law & Security Report, (Elsevier Science) at 275

I. S. Rubinstein, "Export Controls on Encryption Software" (1995). in INTERNATIONAL CRYPTOGRAPHIC INSTITUTE 1995: GLOBAL CHALLENGES 11-12

"Frauded," *San Jose Mercury News*, (14 December 1984)

B. Schneider, "One-Way Hash Functions", (Sept 1991), Dr Jobb's Journal (New York, Miller Freeman, 1991) at 151

"Wassenaar-aftalen indført i Danmark" Lov & Data, Nr 59, September 1999 at 18

M.J. Wiener. "Efficient DES Key Search" presented at the CRYPTO rump session in August 1993, TR-244, School of Computer Science, Carleton University (May 1994)

P. Williams, "Transnational Criminal Organizations and International Security," (1994) 36, Survical, 1

NOTES, UNPUBLISHED MANUSCRIPTS ETC,

E.R. Cummings, Note, Panel discussion of the American Society of International Law (ASIL) Remarks by Cummings, E.R. 89 *Proc. ASIL* (1995), (when discussing the characteristics of the Wassenaar Arrangement)

ELECTRONIC MEDIA

"About TRUSTe", Http://www.etrust.com/webpublishers/about.html

"Bert-Jaap Koops Crypto Law Survey" (September 1997)
http://www.cwis.kub.nl/~frw/people/koops/cls2.htm#co

"Bernstein v. USDOJ" (August 2000)
http://www.steptoe.com/webdocs.nsf/files/bernstein/$file/bernstein.html

"R.H. Brown, chair National Information Infrastructure Task Force", Speech (15 September 1993), National Information Infrastructure Agenda for Action. Available online at http://www.iitf.nist.gov/documents/speeches/brown.html (date accessed: 4 July 1997)

"Commercial encryption export controls", http//www.bxa.doc.gov/encryption.htm

"Crypto", Http://www.iya.com/nrc03.txt

"Cryptographic Products", http://www.tis.com/crypto/crypto-survey.html.

"Cryptography's Role in Securing the Information Society'' National Research Council's Report –NRC-, http://www.replay.com/mirror/nrc (30 May 1996) (prepublication copy which is marked "Subject to further Editorial correction.")

"Cryptography's Role in Securing the Information Society", November 1996, http://www4.nas.edu/cpsma/cstbweb.nsf/86e5876b3bf8be848525631f00688fc5/7a7b246615687e1c8525633a005c4153?OpenDocument" Comments of June 11, 1996 of the NRC Cryptography Report, May 1996".

"Decoding the OECD's Guidelines for Cryptography Policy" (1997), http://www.steptoe.com/comment.htm,

J. Deutch "Goals", (1997) http://www.nsa.gov:8080/programs/ncs21/goal1.html,

"Development of surveillance technology and risk of abuse of economic information" (December 1999), http://www.gn.apc.org/duncan/stoa_cover.htm,

"Development of surveillance technology and risk of abuse of economic information", http://www.gn.apc.org/duncan/stoa_cover.htm,

"Discours et Interventions" (1999), http://.premier-ministre.gouv.fr/PM/D1901999.htm,

"Draft convention for the modernization of the Warsaw system of air carrier liability approved" (2000) http://www.icao.org/icao/en/nr/pio9709.htm

"Dual-Use list- Category 5-Part II- Information Security" (http://www.wassenaar.org/docs.html)

"Electronic Time-Stamping: The Notary Public Goes Digital"(1997), http://www.surety.com

"Encryption Policy and Market Trends" , http://www.cosc.georgetown.edu/~denning/crypto/trends.html

"Europe to Drive Online Boom", http://www.wired.com/news/"business/story/14511.html

"Facts and figures" (1998), http://www.nsa.gov:8080/about/

"Feds relax crypto rules" (Wired Magazine, September 1998), http://www.wired.com./news/news/politics/story/15037.html

"General presentation" (October 1998) http://www.stategis.ic.gc.ca/html

"Inför en svensk policy för säker elektronisk kommunikation, Rapport 6/97, SOU 1997:73" http://www.itkommissionen.se/PDF/rapp9706.pdf.

"Inside the NSA" (1998), http://www.nsa.giv:8080/docs/cuba/index.html

"Is Encryption Speech? - A Cryptographer's Perspective" (1998), http://www.cosc.georgetown.edu/~denning/crypto.

" It Came From Planet Clipper: The Battle over Cryptographic Key "Escrow"(1 November 1996), http://www.law.miami.edu/~froomkin/articles/planet_clipper.htm

"Law enforcement in Cyberspace", Conference to the Commonwealth Club of California (June 14, 1996), http://guru.cosc.georgetown.edu/~denning/Reno-commonwealth.txt

Letter from a working group, compromised of representatives of the Federal Bureau of Investigation, National Security Agency and the Department of justice to Mr. George Tenet, Special Assistant to the President and Senior Director for Intelligence Programs, (9 February 1993) (http://www.epic.org)

"Nua Internet Surveys", http://www.nua.ie/surveys

"Navidec Inc: 53 percent of US Users Have Bought Online" (1 July 1999), http://www.nua.ie/surveys/index.cgi?VS&art_id=905355027&rel=true

"NSA and the Cuban Missile Crisis" (1999) http://www.nsa.gov:8080/docs/cuba/index.html

"Pretty Poor Privacy", Wired (28 June 1998), http://www.wired.com/news/politics/story/13256.html

"Privacy Protection on Global networks", http://www.oecd//dsti/sti/it/secur/act/privnote.htm..

"Public Statement" regarding the Wassenaar Arrangement On Export Controls for Conventional Arms and Dual-Use Goods and Technology, Vienna, 3 December 1998, http://www.wassenaar.org/docs/press_4.html

E. Ratcliff, "Spying on the Echelon Spy Network" (2000), Wired Magazine, online: Wired Magazine http://www.wired.com/archeive/8.04/mustread.html?pg=2

Recommendation No. R (95) 13 of the Committee of Ministers to Member States Concerning Problems of Criminal Procedure Law Connected with Information Technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543 meeting of the Ministers' Deputies) http://www.privacy.org/pi/intl_orgs/coe/info_tech_1995.html

"Re-Evaluating Proposals for a Public Key Infrastructure" (1995) http://www.law.mcgill.ca/coursenotes/complaw/papers/1995-pki.htm.

"Report on Background and Issues of Cryptography Policy" (1997), http://www.oecd.org/dsti/iccp/legal/cryptopol.htm,

"Ripe Network Coordination Centre", http://www.ripe.net/statistics/hostcount.html

"RSA Security" (18 August 2000) Http://www.rsa.com (date accessed: 18 August 2000)

"Shopping behavior in the age of interactivity" (1 July 1999), http://www.1to1.com/articles/i1-070199/cdirect.html,

"Shop.org: Online retailing to Top USD 36 Billion in 1999", (1 July 1999) http://www.nua.ie/survesy/index.cgi?f=VS&art_id=90535503&rel=true

"Spying on the Spies" (Wired 10 May 1999), http://www.wired.com/wired/archive/5.08/spy.html?pg=6&topic=

"The Cryptography Project", http://www.cosc.georgetown.edu/~denning/crypto

"The Crisis Grows" (1999), http://www.nsa.gov:8080/docs/cuba/index.html

"The Final Report of the National Research Council" Http://www.replay.com/mirror/nrc/nrc07.txt.

"The History of the Wassenaar Arrangement" (1999), http://www.org/docs/history.html

"The President's Commission on Critical Information Infrastructure (PCCIP)" http://www.info-sec.com/pccip/web/index.html

"The Verona Project" (1998), http://www.nsa.gov:8080/docs/Verona/ddir.html,

"The Wassenaar Arrangement" (1999) http://www.wassenaar.org/docs/talkpts.html

"Towards An European Framework for Digital Signatures and Encryption" (1997), http://www.ipso.cec.be/eif/policy/97503.html,

"Wassenaar" (1999), http://www.wassenaar.org/docs/History.html

"White House Fact Sheet; Administration Updates Encryption Export Policy", http://www.steptoe.com/webdoc.nsf/83/doc6dc16e7abd3852659f00499doq/10cfb7b70e573152852567f3005a07b5?Open Document. (The White House, Office of the Press Secretary, 16 September, 1999)

"Workshop on Privacy Protection in a Global Networked Society" (1998), http://www.oecd.org//dsti/sti/it/secur/prod/reg98-5final.pdf.

"Work in Progress" (October 1998), http://www.stategis.ic.gc.ca/ottawaoecdconference/ott_wip.htm.

"United Nations Manual on the Prevention and Control of Computer- Related Crime"
http://www.ifs.unvie.ac.at/~pr2gq1/rev4344.html

DEFINITIONS

"Authentication" means a function for establishing the validity of a claimed identity of a user, device or another entity in an information or communications system.
"Availability" means the property that data, information, and
information and communications systems are accessible and usable on a timely basis in the required manner.
"Confidentiality" means the property that data or information is not made available or disclosed to unauthorized individuals, entities, or processes.
"Cryptography" means the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorized use.
"Cryptographic key" means a parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.
"Cryptographic methods" means cryptographic techniques, services, systems, products and key management systems.
"Data" means the representation of information in a manner suitable for communication, interpretation, storage, or processing.
"Decryption" means the inverse function of encryption.
"Encryption" means the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.
"Integrity" means the property that data or information has not been modified or altered in an unauthorized manner.
"Interoperability" of cryptographic methods means the technical ability of multiple cryptographic methods to function together.
"Key management system" means a system for generation, storage, distribution, revocation, deletion, archiving, certification or application of cryptographic keys.
"Keyholder" means an individual or entity in possession or control of cryptographic keys. A keyholder is not necessarily a user of the key.
"Law enforcement" or "enforcement of laws" refers to the enforcement of all laws, without regard to subject matter.
"Lawful access" means access by third party individuals or entities, including governments, to plaintext, or cryptographic keys, of encrypted data, in accordance with law.
"Mobility" of cryptographic methods only means the technical ability to function in multiple countries or information and communications infrastructures.
"Non-repudiation" means a property achieved through cryptographic methods, which prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection of authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership).
"Personal data" means any information relating to an identified or identifiable individual.
"Plaintext" means intelligible data.
"Portability" of cryptographic methods means the technical ability to be adapted and function in multiple systems.

ABBREVIATIONS AND ACRONYMS

AECA –	Arms Export Control Act
Art	Article

BBS –	An electronic bulletin board
CA –	Certification Authority, an authority set up to verify that a the keys registered in the database at the authority belongs to the registered keyholders. It issues a certificate as proof of this. Sometimes called TTP- Trusted Third Party
CD-Rom	Compact Disc with Read Only memory
COCOM	Coordinating Committee on Multilateral Export Controls
Comint	Communication Intelligence
CRL-	Certification Revocation List: a list of with revoked certificates issued for public keys
Crypto	Cryptography
Cryptographic Algorithm-	A mathematical function encrypts of decrypts information. This is the heart of a cryptographic program.
Digital Signature	An electronic signature created by an cryptographic algorithm in the form of a checksum
EC	European Communities (precursor to the European Union)
EC	European Community
EDI	Electronic Data Interchange, electronic exchange of documents and orders between two or several parties
Encryption	scrambling of data by a cryptographic algorithm that makes it incomprehensible without decryption
EU	European Union
EU	European Union
GII	Global Information Infrastructure: It was initially an initiative by the G7 countries to enhance the global information infrastructure
Hertz	A measurement for cycles per second
Humint	Human Intelligence
ICAO	International Civil Aviation Review
ISO	The International Organization for Standardization
ITAR	International Traffics in Arms Regulation (US)
ITU	The International Telecommunications Union
Key escrow	A initiative to held private keys at one or several custodians. Originally launched by the USA.
NATO	North Atlantic Treaty Organization
NBC	Nucelar, Biological and Chemical[Weapons]
NJA	Nytt Juridiskt Arkiv, Avd I (Swedish Supreme Court Reports)
OECD	The Organization for Economic Cooperation and Development
OECD	Organization for Economic Cooperation and Development
PGP	Pretty Good Privacy, an encryption software program developed by Paul Zimmerman. Instead of using CAs to verify the connection between the keyholder and the public key a web of trust is created that enabled users to verify other users.
Photoint	Photographic Intelligence
PKI	Public Key Infrastructure
Prop	Proposition (Legislative Bill)
RSA	The initials stands for Rivest, Shamir and Adleman who created an encryption program called RSA
SET	Secure Electronic Transaction- a system for secure online transactions. Supported by VISA.
SFS	Svensk Författningssamling (Swedish Book of Statutes)
Sigint	Signals Intelligence
SOU	Statens Offentliga Utredningar (Public Investigations of the State)
SvJt	Svensk Juristtidning

APPENDIX – OECD GUIDELINES FOR CRYPTOGRAPHY POLICY

I. AIMS

The Guidelines are intended:

to promote the use of cryptography;
to foster confidence in information and communications infrastructures, networks and systems and the manner in which
they are used;
to help ensure the security of data, and to protect privacy, in national and global information and communications
infrastructures, networks and systems;
to promote this use of cryptography without unduly jeopardising public safety, law enforcement, and national security;
to raise awareness of the need for compatible cryptography policies and laws, as well as the need for interoperable,
portable and mobile cryptographic methods in national and global information and communications networks;
to assist decision-makers in the public and private sectors in developing and implementing coherent national and
international policies, methods, measures, practices and procedures for the effective use of cryptography;
to promote co-operation between the public and private sectors in the development and implementation of national and
international cryptography policies, methods, measures, practices and procedures;
to facilitate international trade by promoting cost-effective, interoperable, portable and mobile cryptographic systems;
to promote international co-operation among governments, business and research communities, and standards-making
bodies in achieving co-ordinated use of cryptographic methods.

II. SCOPE

The Guidelines are primarily aimed at governments, in terms of the policy recommendations herein, but with anticipation that
they will be widely read and followed by both the private and public sectors.

It is recognised that governments have separable and distinct responsibilities for the protection of information which requires
security in the national interest; the Guidelines are not intended for application in these matters.

III. DEFINITIONS

For the purposes of the Guidelines:

"Authentication" means a function for establishing the validity of a claimed identity of a user, device or another entity in an
information or communications system.
"Availability" means the property that data, information, and information and communications systems are accessible and
usable on a timely basis in the required manner
"Confidentiality" means the property that data or information is not made available or disclosed to unauthorised

individuals, entities, or processes.

"Cryptography" means the discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, establish its authenticity, prevent its undetected modification, prevent its repudiation, and/or prevent its unauthorised use.

"Cryptographic key" means a parameter used with a cryptographic algorithm to transform, validate, authenticate, encrypt or decrypt data.

"Cryptographic methods" means cryptographic techniques, services, systems, products and key management systems.

"Data" means the representation of information in a manner suitable for communication, interpretation, storage, or processing.

"Decryption" means the inverse function of encryption.

"Encryption" means the transformation of data by the use of cryptography to produce unintelligible data (encrypted data) to ensure its confidentiality.

"Integrity" means the property that data or information has not been modified or altered in an unauthorised manner.

"Interoperability" of cryptographic methods means the technical ability of multiple cryptographic methods to function together.

"Key management system" means a system for generation, storage, distribution, revocation, deletion, archiving, certification or application of cryptographic keys.

"Keyholder" means an individual or entity in possession or control of cryptographic keys. A keyholder is not necessarily a user of the key.

"Law enforcement" or "enforcement of laws" refers to the enforcement of all laws, without regard to subject matter.

"Lawful access" means access by third party individuals or entities, including governments, to plaintext, or cryptographic keys, of encrypted data, in accordance with law.

"Mobility" of cryptographic methods only means the technical ability to function in multiple countries or information and communications infrastructures.

"Non-repudiation" means a property achieved through cryptographic methods, which prevents an individual or entity from denying having performed a particular action related to data (such as mechanisms for non-rejection of authority (origin); for proof of obligation, intent, or commitment; or for proof of ownership).

"Personal data" means any information relating to an identified or identifiable individual.

"Plaintext" means intelligible data.

"Portability" of cryptographic methods means the technical ability to be adapted and function in multiple systems.

IV. INTEGRATION

The principles in Section V of this Annex, each of which addresses an important policy concern, are interdependent and should be implemented as a whole so as to balance the various interests at stake. No principle should be implemented in isolation from the rest.

V. PRINCIPLES

1. TRUST IN CRYPTOGRAPHIC METHODS

Cryptographic methods should be trustworthy in order to generate confidence in the use of information and communications systems.

Market forces should serve to build trust in reliable systems, and government regulation, licensing, and use of cryptographic methods may also encourage user trust. Evaluation of cryptographic methods, especially against market-accepted criteria, could also generate user trust.

In the interests of user trust, a contract dealing with the use of a key management system should indicate the jurisdiction whose laws apply to that system.

2. CHOICE OF CRYPTOGRAPHIC METHODS

Users should have a right to choose any cryptographic method, subject to applicable law.

Users should have access to cryptography that meets their needs, so that they can trust in the security of information and communications systems, and the confidentiality and integrity of data on those systems. Individuals or entities who own, control, access, use or store data may have a responsibility to protect the confidentiality and integrity of such data, and may therefore be responsible for using appropriate cryptographic methods. It is expected that a variety of cryptographic methods may be needed to fulfil different data security requirements. Users of cryptography should be free, subject to applicable law, to determine the type and level of data security needed, and to select and implement appropriate cryptographic methods, including a key management system that suits their needs.

In order to protect an identified public interest, such as the protection of personal data or electronic commerce, governments may implement policies requiring cryptographic methods to achieve a sufficient level of protection.

Government controls on cryptographic methods should be no more than are essential to the discharge of government responsibilities and should respect user choice to the greatest extent possible. This principle should not be interpreted as implying that governments should initiate legislation which limits user choice.

3. MARKET DRIVEN DEVELOPMENT OF CRYPTOGRAPHIC METHODS

Cryptographic methods should be developed in response to the needs, demands and responsibilities of individuals, businesses and governments.

The development and provision of cryptographic methods should be determined by the market in an open and competitive environment. Such an approach would best ensure that solutions keep pace with changing technology, the demands of users

and evolving threats to information and communications systems security. The development of international technical standards,
criteria and protocols related to cryptographic methods should also be market driven. Governments should encourage and
co-operate with business and the research community in the development of cryptographic methods.

4. STANDARDS FOR CRYPTOGRAPHIC METHODS

Technical standards, criteria and protocols for cryptographic methods should be developed and promulgated at the
national and international level.

In response to the needs of the market, internationally-recognised standards-making bodies, governments, business and other
relevant experts should share information and collaborate to develop and promulgate interoperable technical standards, criteria
and protocols for cryptographic methods. National standards for cryptographic methods, if any, should be consistent with
international standards to facilitate global interoperability, portability and mobility. Mechanisms to evaluate conformity to such
technical

standards, criteria and protocols for interoperability, portability and mobility of cryptographic methods should be developed.
To the extent that testing of conformity to, or evaluation of, standards may occur, the broad acceptance of such results should
be encouraged.

5. PROTECTION OF PRIVACY AND PERSONAL DATA

The fundamental rights of individuals to privacy, including secrecy of communications and protection of personal
data, should be respected in national cryptography policies and in the implementation and use of cryptographic
methods.

Cryptographic methods can be a valuable tool for the protection of privacy, including both the confidentiality of data and
communications and the protection of the identity of individuals. Cryptographic methods also offer new opportunities to
minimise the collection of personal data, by enabling secure but anonymous payments, transactions and interactions. At the
same time, cryptographic methods to ensure the integrity of data in electronic transactions raise privacy implications. These
implications, which include the collection of personal data and the creation of systems for personal identification, should be
considered and explained, and, where appropriate, privacy safeguards should be established.

The OECD Guidelines for the Protection of Privacy and Transborder Flows of Personal Data provide general guidance
concerning the collection and management of personal information, and should be applied in concert with relevant national law
when implementing cryptographic methods.

6. LAWFUL ACCESS

National cryptography policies may allow lawful access to plaintext, or cryptographic keys, of encrypted data.
These policies must respect the other principles contained in the guidelines to the greatest extent possible.

If considering policies on cryptographic methods that provide for lawful access, governments should carefully weigh the
benefits, including the benefits for public safety, law enforcement and national security, as well as the risks of misuse, the
additional expense of any supporting infrastructure, the prospects of technical failure, and other costs. This principle should not
be interpreted as implying that governments should, or should not, initiate legislation that would allow lawful access.

Where access to the plaintext, or cryptographic keys, of encrypted data is requested under lawful process, the individual or
entity requesting access must have a legal right to possession of the plaintext, and once obtained the data must only be used for
lawful purposes. The process through which lawful access is obtained should be recorded, so that the disclosure of the
cryptographic keys or the data can be audited or reviewed in accordance with national law. Where lawful access is requested
and obtained, such access should be granted within designated time limits appropriate to the circumstances. The conditions of
lawful access should be stated clearly and published in a way that they are easily available to users, keyholders and providers of
cryptographic methods.

Key management systems could provide a basis for a possible solution which could balance the interest of users and law
enforcement authorities; these techniques could also be used to recover data, when keys are lost. Processes for lawful access
to cryptographic keys must recognise the distinction between keys which are used to protect confidentiality and keys which are
used for other purposes only. A cryptographic key that provides for identity or integrity only (as distinct from a cryptographic
key that verifies identity or integrity only) should not be made available without the consent of the individual or entity in lawful
possession of that key.

7. LIABILITY

Whether established by contract or legislation, the liability of individuals and entities that offer cryptographic
services or hold or access cryptographic keys should be clearly stated.

The liability of any individual or entity, including a government entity, that offers cryptographic services or holds or has access to
cryptographic keys, should be made clear by contract or where appropriate by national legislation or international agreement.
The liability of users for misuse of their own keys should also be made clear. A keyholder should not be held liable for
providing cryptographic keys or plaintext of encrypted data in accordance with lawful access. The party that obtains lawful
access should be liable for misuse of cryptographic keys or plaintext that it has obtained.

8. INTERNATIONAL CO-OPERATION

Governments should co-operate to co-ordinate cryptography policies. As part of this effort, governments should remove, or avoid creating in the name of cryptography policy, unjustified obstacles to trade.

In order to promote the broad international acceptance of cryptography and enable the full potential of the national and global information and communications networks, cryptography policies adopted by a country should be co-ordinated as much as possible with similar policies of other countries. To that end, the Guidelines should be used for national policy formulation.

If developed, national key management systems must, where appropriate, allow for international use of cryptography.

Lawful access across national borders may be achieved through bilateral and multilateral co-operation and agreement.

No government should impede the free flow of encrypted data passing through its jurisdiction merely on the basis of cryptography policy.

In order to promote international trade, governments should avoid developing cryptography policies and practices which create unjustified obstacles to global electronic commerce. Governments should avoid creating unjustified obstacles to international availability of cryptographic methods.