HCLT Publications Series

Issue No. 1

Fighting Terror Online

By

The Students of the Multidisciplinary Workshop in Law & Technology

Haifa, 2002
Multidisciplinary Workshop in Law and Technology
The Haifa Center of Law and Technology
Faculty of Law
University of Haifa

Authors
Eran Aloni
Rahel Aridor
Eran Bar-Or
Yael Bergman
Udi Einhorn
Keren Elisha
Gal Eschet
Alon Fiul
Haviva German
Eyal Greener
Shahar Grinberg
Efy Michaeli
Tal Ron
Nir Segal
Miri Shai
Asaf Zabari
Ben Zohar

Advisors and Editors
Dr. Michael D. Birnback
Dr. Niva Elkin-Koren

With the assistance of the Caesarea Edmond Benjamin de Rothschild
Foundation Institute for Interdisciplinary Applications of Computer Science

Translation
Stephanie Nakache
Perry Zamek

ISBN 965-90924-0-7
Foreword and Acknowledgements

The events that took place in the fall of 2001 led legislators and governments throughout the world to reconsider their policies regarding security issues. Among its many tools, global terror also uses advanced technological methods, and this presents a difficult challenge to policymakers. It is on this basis that we decided to dedicate the 2002 Research Workshop in Law and Technology to the issue of formulating appropriate policy at the interface between security and technology, human rights and economic policy. Participating in the workshop were seventeen outstanding students from Haifa University’s Faculty of Law, who had been specifically chosen to join the workshop.

The Workshop in Law and Technology is a unique research framework that deals with practical questions in the area of information policy. Policy formulation in the area of law and technology occurs not only in the courts, but also – and perhaps to a greater extent – in the Knesset (Israeli Parliament) and within the various State authorities. Policymakers need information, data, evaluations, and analyses of the significance and implications of policy, and these form the basis for decisions as to future directions. For the most part, however, this information is provided by interest groups, whose data reflect and promote their particular interests. The public voice is almost never heard in these discussions. Companies too – in particular, new start-ups – need legal guidance when it comes to issues with public implications. The Workshop in Law and Technology is designed to fill this gap.

The research and writing effort in the workshop went through a number of phases. After initial brainstorming and formulation of the issues for research, participant students were divided into teams working on various aspects of the research: one team focused on technological issues, another on legal issues, while a third team ranged further field, into areas such as strategic studies, economics, communications and media, and so on. The initial research phase was followed by a number of sessions with workshop participants, under our guidance, at which the questions and issues under discussion were elucidated. With completion of the research stage and the writing of an initial draft of the position paper, we felt that it would be appropriate to learn about the views of experts and professionals working in the areas that we had
dealt with. And so the Shefayim Conference (26-27 December 2001) came into being. For two intense days, we discussed the issues with dozens of experts from various areas of research and activity: computer science, law, communications and media, strategic studies, and so on. Lawyers and jurists came from academia, from the private sector, and from the public sector – from the Ministry of Justice, the Ministry of Defense and the Ministry of Communication. We also heard the opinions of those who are directly involved: researchers in the field of encryption defense personnel, lawyers and businessmen. The dynamic that was created over the two days of discussions, informative lectures and fruitful discussions, made absolutely clear the need for independent discussion and interdisciplinary research on issues related to law and technology.

The conclusions drawn from the research and the Shefayim Conference are summarized in the position paper before you. In many instances, this is the first attempt to deal with issues that have not yet been discussed publicly in Israel. It is our hope that this position paper will serve as the basis for serious discussion of issues that need to be resolved, and will assist in the formulation of an intelligent policy response in the war against terror on-line.

The activities of the Workshop could only take place thanks to the generous support of the Caesarea Edmond Benjamin de Rothschild Foundation Institute for Interdisciplinary Applications of Computer Science at the University of Haifa. We would like to express our appreciation to the Institute’s director, Professor Martin Golumbic, and its scientific coordinator, Dr. Irith Hartman, who not only provided us with the means, but also showed enthusiasm throughout the project, and were active contributors to the conference itself. Our thanks also to Ms. Sheryl Zorella, the Institute’s administrative coordinator, for her enormous assistance in preparing for the Shefayim Conference.

A distinguished list of experts contributed time and energy to the workshop, and all the participants made valuable contributions. The participants gave focus to the questions under discussion, presented a range of viewpoints regarding the issues on the agenda, and offered a clearer perspective on points that were still blurry. We would like to thank all of them (in alphabetic order):
Dr. Gadi Aharoni; Adv. Amit Ashkenazi; Adv. Mike Blass; Adv. Mati Barzam; Karine Barzilai-Nahon; Adv. Nava Ben Or; Professor Ariel Bendor; Adv. Tamar Calahora; Mr. Yoram Cohen; Dr. Moshe Cohen-Elya; Professor Rafi Cohen-Almagor; Professor Emmanuel Gross; Shimon Gruper; Adv. Boaz Guttman; Adv. Dorit Inbar; Dr. Yuval Karniel; Adv. Sharon Keren; Professor Hugo Krawczyk; Professor Eyal Kushilevitz; Dr. Hillel Nosek; Mr. Ariel Pizetzky; Professor Sheizaf Rafaeli; Adv. Haim Ravia; Adv. Ram Raviv; Adv. Dudi Salmanovitch; Yael Shahar; Yosi Shani; Efrat Shimoni; Dr. Ariel Sobelman; Adv. Tana Spanitz; Eric Wolf; Dr. Limor Yagil; Dr. Asaf Yakov; Dr. Yariv Zfat.

During the course of the research, writing and preparation of the workshop, we consulted with additional people, and we would also like to thank them: Professor Niv Ahituv; Oded Cohen; Dr. Amos Fiat; Dr. Dafna Lamish; Dr. Fania Oz-Salzberger; Professor Gabi Weimann.

Our thanks, too, to the members and staff of the Faculty of Law, University of Haifa, who assisted us: the Dean, Professor Joseph Edrey; the faculty’s Director of Administration, Moshe Sayag; Faculty Coordinator, Dorit Arbel; and the Dean’s secretary, Dassi Fisher. The production of the conference could not have taken place without the dedicated work of Tal Ron, the coordinator of the Law and Technology Center.

Niva Elkin-Koren, Michael Birnhack
Haifa, September 2002
### CONTENTS

- Detailed Table of Contents
- Summary of Findings and Recommendations

I. Preface: Security Concerns – Mapping the Threats


TABLE OF CONTENTS

Foreword and Acknowledgements ..................................................................................................3
Summary of Findings and Recommendations ...............................................................................2
I. Preface: Security Concerns – Mapping the Threats ..............................................................1
   A. The Problem ....................................................................................................................9
   B. What is Encryption? The Technological Basis ..............................................................10
      1. Preface ...................................................................................................................10
      2. The Basic Principle of Encryption: Letter Replacement ..........................................12
      3. Symmetrical Encryption .......................................................................................12
      4. Asymmetrical Encryption: Public Key and Private Key .........................................14
   C. Security Needs .............................................................................................................19
      1. Data Protection .......................................................................................................20
      2. Monitoring – Intelligence .....................................................................................21
      3. The Rationale for Regulation .................................................................................23
   D. The Legal Framework ..................................................................................................24
      1. Israel: From Blanket Prohibition to Prior Licensing and Subsequent Control 24
      2. United States .........................................................................................................33
      3. The International Scene .......................................................................................38
      4. The International Scene – Decryption ..................................................................44
   E. Implications and Policy Considerations .........................................................................53
      1. Market Intervention and Research and Development Considerations ...............53
         a. The influence of governmental intervention on research and development 53
         b. Restrictions on export of the means of encryption and the use thereof ..........54
      2. The Influence of Encryption Regulation on Electronic Commerce ..................56
      3. The Right to Privacy .............................................................................................56
      4. Freedom of Speech ..............................................................................................60
      5. Freedom of Occupation .......................................................................................67
      6. Property Rights ....................................................................................................72
   F. Summary of Recommendations ......................................................................................73
III. Online Monitoring: Security, Privacy and Freedom of Speech ........................................77
   A. Introduction ...............................................................................................................77
   B. Intelligence in the Information Age .............................................................................79
      1. General Background .............................................................................................79
      2. Means of Collecting Information and Monitoring the Internet ..........................81
         2.1 Information Monitoring ..................................................................................82
      2.2. Collection of Information on the Server or the PC .........................................85
   C. Prevention and Enforcement in the Information Age and human rights .....................88
      1. Foreword ...............................................................................................................88
      2. What is privacy and what is the right to privacy? ...............................................88
      3. Is protection of privacy on-line justified? .........................................................89
      4. What are the limits of the protection of privacy in the information age? .......93
   D. Legal Limitations on Acts of Prevention and Enforcement in the Information Age ....97
      1. The Legal Framework ..........................................................................................97
      2. The International Context ....................................................................................98
         2.1 Protection of the Right to Privacy ...................................................................98
         2.2 International Regulation for Protection of Personal Data ...............................99
3. The European Union ................................................................. 102
  3.1 The EU Directive on Data Protection ..................................... 103
  3.2 Implementation of the Directive by the Member States .......... 104
  3.3. Legal Developments after September 11 .............................. 105
  3.4 The New British Anti-Terrorism Act ................................. 107
  3.5 Data Collection by ISP’s ...................................................... 107
4. The USA .............................................................................. 111
  4.1 General Background ........................................................... 111
  4.2 Legal control of invasion of privacy by the enforcement agencies .. 113
5. Other Countries ..................................................................... 116
  5.1 Canada ............................................................................ 116
  5.2 Australia .......................................................................... 117
E. The Legal Framework: Israel ....................................................... 118
  1. Introduction .......................................................................... 118
  2. Enforcement .......................................................................... 120
  3. Search And Seize .................................................................... 122
  4. Secret Monitoring in Israeli Law ............................................. 124
  5. Liability of Internet Service Providers ................................... 134
F. The Information Age: Is there a Need for New Regulation ........ 135
  1. Is the existing system of checks and balances suited to the Internet? .... 135
  2. What is the significance of implementation of the existing legal regulation to the Internet? .......................... 137
G. Summary of Recommendations .................................................. 138
IV. Online Propaganda: Security, Freedom of Speech and Service Providers’ Liability Issues ......................................................... 139
A. What is .................................................................................. 139
  1. Propaganda Terror versus Propaganda in the Service of Terror .......... 139
  2. Contents of the Propaganda ..................................................... 140
  3. Propaganda Methods ............................................................... 142
  4. Does the medium change the nature? Psychological warfare in the technological age .................. 142
B. Freedom of Speech on the Internet ............................................. 144
C. Liability of providers ................................................................ 147
  1. Considerations in placing liability on intermediate agencies (service providers) .................. 148
    a. Model of Liability .............................................................. 151
    b. Full Immunity .................................................................... 152
    c. Conditional and Restricted Liability .................................... 153
  3. The Legal Situation In Israel .................................................... 154
D. Summary of Recommendations .................................................. 155
Summary of Findings and Recommendations
I. Preface: Security Concerns – Mapping the Threats

As we enter the third millennium, the digital environment plays a key role in our lives. It is not just a public marketplace, or an infinite repository of information. A growing segment of human activity today takes place in that environment: interpersonal communications, commerce, management and control of essential infrastructure systems, research, and more. However, this environment has also become a battlefront, as the events of September 11 have so clearly shown.

Over recent years, legal systems, both in Israel and overseas, have struggled with the need to adapt rules and concepts, which were developed in the context of a “concrete” world, to the “virtual” environment. The questions dealt with by legislators; courts and researchers mainly concerned commercial contexts, such as adapting intellectual property and privacy laws to the new medium, or criminal contexts, such as gambling and the fight against pedophilia. Today, worldwide attention is being given to new security threats, in the form of global terrorism. Legal systems are being called upon to provide a response to these threats, in all areas of life, including the on-line environment. The fundamental issue – the tension between security needs and civil rights – is not new. A great deal of experience has been amassed in various countries regarding these issues. The question that now arises is, whether the existing system of principles and laws, developed on the basis of experience gathered in the “concrete” world, is applicable to the digital environment.

The present position paper will show that the on-line environment is a significant and relevant arena of activity in the fight against terror, and will identify the threats, the security needs, and the issues that are unique to this environment. We will examine whether the unique characteristics of this environment require new legal solutions, or whether existing solutions are sufficient. We will expand upon three areas of on-line activity that require reexamination: encryption, monitoring, and propaganda. For each of these, we will indicate the issues, examine existing legal arrangements in Israel and overseas, and offer guidelines for formulating legal policy.

---

1 In preparing this chapter we were greatly assisted by lectures given by Shimon Gruper, Eric Wolf, Dr. Ariel Sobelman, Ariel Pizetzky, Yael Shahar, and Yosi Shani, and to them we offer our thanks. Responsibility for the content, of course, is all our own.
In the following pages, we will demonstrate the need to address the digital environment as a battlefront, map the new security threats, and thereby focus the discussion.

**Mapping the Threats**

Formulation of an appropriate legal policy at the interface between security, technology, human rights and economic policy is impossible, unless we recognize the security threats faced by states and individuals, the resulting security needs, and existing countermeasures. Discussions of national security strategy usually deals with questions of power buildup, composition of forces, strength in military, economic and morale terms, identification of vulnerabilities, relative and absolute advantages, and threat analysis. We can divide security threats into two types:

1. **Existential threat** – a threat that may undermine a state, or at least lead to heavy loss of life and/or extensive damage to strategic assets and national infrastructure. In general, this type of threat is posed by states with an organized military structure. In the United States, nuclear war is generally viewed as an existential threat. In Israel, such a threat would be presented by an all-out war with neighboring Arab states, such as the Yom Kippur War.

2. **Nuisance threat** – a threat that may cause loss of life or damage to materiel, but not to the extent that it would pose a threat to the existence of the state. Generally, this applies to terrorist acts carried out by non-state organizations (although some are supported by states) with the aim of achieving political goals.

Of course, this is not a simple binary scale: between these two extremes one might identify threats at various intermediate levels. The terror attacks of September 11, 2001 turned the threat of terror in the international arena from the nuisance level to a level close to that of an existential threat. The murder of thousands of people within a matter of minutes, and the critical damage, both economic and symbolic, to the nerve centers of the international economy and the American defense establishment, were much closer, at least in terms of effect, to the detonation of a nuclear bomb, than to
any localized terror attack. The danger of biological terror and the fear that terrorist organizations may gain control over nuclear weapons emphasize the increasing importance of the terrorist threat. It may therefore be concluded that the importance of the distinction between state-based threats and non-state terror threats, or between existential and nuisance threats, has lessened. As we will explain below, this fact takes on renewed significance when we discuss the use of technological tools in the realm of computer and communications systems.

**Information Warfare**

The present paper will focus solely on those security considerations relevant to computer and communications systems. Computer communications systems may themselves serve as a battleground; in the common terminology, this is known as Information Warfare.² This is a broad concept, which also includes cyberterrorism. The Israeli State Comptroller’s Report for 2001 defines this as “carrying out acts, whose aim is to damage the enemy’s computer systems (aggressive information warfare) while defending your own computer systems (defensive information warfare). The most common forms of attack are theft of data and information (damage to secrecy), interruptions and destruction (damage to reliability and availability), and damage to electronic installations, their disruption and destruction (damage to reliability and availability). One of the basic scenarios in aggressive information warfare is an attack against a number of essential computer systems simultaneously.”³

Attacks may be carried out by a whole spectrum of harmful and destructive programs⁴: viruses,⁵ worms,⁶ Trojan horses,⁷ logic bombs,⁸ back doors (trap doors),⁹

---

⁴ For further information, see: Dorothy Denning & Frank Drake, “A Dialog on Hacking and Security” in Computers, Ethics and Social Values 120-125 (Deborah G. Johnson & Helen Nissenbaum eds., NJ, 1995).
⁵ “A computer virus is a program like any other, but, unlike other programs, computer viruses are designed to copy themselves into other programs. Also, unlike regular programs, the aim of the virus is
as well as hardware components. These methods are aimed against a range of targets. One of the key vulnerabilities of Western society in the information age is the information systems of national infrastructures: logistics, finance, health, water, electricity, communications, etc. This is both because of society’s heavy reliance on information systems, and because of the interconnectedness of those systems through a network that is open to the public. Computer systems are, by their nature, service providers. The more essential a service is for the state’s economy and its properly to damage programs residing on the computer. When the user runs a program infected by a virus, then the virus code is also run, and this may contain commands that may damage files on the computer or even delete them.” See Yochai Sharon, “HaAtar HaIvri HaRishon BeNose Virusim [The First Israeli Site on the Topic of Viruses]” http://www.cs.biu.ac.il/~yohais1/faq.html#1.

A worm is an independent program that copies itself from computer to computer across the Internet, often causing overload on the computers through which it passes. However, unlike viruses, it generally doesn’t cause serious damage. In contrast to viruses, worms are not code fragments that attach themselves to or modify existing files. Rather, they are more like stand-alone programs. The first model of a worm was demonstrated as an experiment in early 1988, and caused a furor in the world of computers. Even if the worm is not itself designed to cause damage, the fact that it uses computer resources leads, in the end, to the computer being slowed down, and this can, in many cases, affect users. For further details, see Peter J. Denning, “The Internet Worm”, American Scientist 126-128 (March-April 1989). The article also appears in Denning’s book, Computers Under Attack 193-200 (New York, 1990).

A Trojan Horse is not a virus, although it has similar characteristics. A Trojan horse is a program which task is to place itself on our computers, while hiding the fact of its own existence, and operate or allow remote operation of certain actions on the computer. Trojan horses of the type we are discussing are introduced surreptitiously through an apparently legal file that might arrive through the Internet, email, or on a diskette. These programs install an agent called a “server.” The agent installs itself silently, and does nothing to reveal its existence. In fact, it does nothing on its own. When we connect to the Internet, our computer is “bombarded” with directed or random probes from penetration programs operated by questionable types. These attempts at penetration are carried out through the communications links to the Internet. When such a program finds its agent (server) installed on the target machine, it allows the interloper to send the target computer commands or messages, ranging from “innocent” messages that pop up and surprise users, to commands that reformat the computer’s hard disks. See: Amir Anavy’s site: “Pinat HaAzarim shel Amir [Amir’s Utilities]”, http://www.anavy.net/util36.html

The idea behind most logic bombs is the misuse of the “Fork” command. This command allows an application to create another copy of itself and to run that copy in parallel. By running a chain of thousands of such commands, the computer’s application table fills up, and in the end the computer grinds to a halt. On application tables and the original uses for which the Fork command was designed, see: Maurice J. Bach, The Design of the Unix Operating System, 192-200 (New Jersey, 1990).

Back doors / trap doors are loopholes in computer systems deliberately left by developers, technicians or systems managers for themselves. Sometimes this refers to loopholes in an encryption method. Back doors allow access to the computer system, often without the need for a user name or password.

Such as, for example, Chipping, a concept related to the introduction of destructive code into processor chips by the manufacturers. The code will run when a given combination of conditions is met, for example, when a certain signal is received at a particular frequency.

functioning, the more it can be considered a “critical infrastructure” of strategic importance. From the strategic value of critical infrastructures we can derive the strategic value of attacking and damaging them.

The response to threats against essential systems can take place on a number of levels. Firstly, at the practical level: in the United States there are a number of authorities whose task is to protect essential infrastructure in general, and computer systems in particular. Among them is the NIPC – National Infrastructure Protection Center,12 and the CIAO – Critical Infrastructure Assurance Office.13 Discussion of this issue in the United States is open, and there is an ongoing dialogue between the government and the private sector. Thus we can find websites and organizations strongly critical of the Administration’s actions in this area, both from the point of view of the curtailment of individual rights, and from the point of view of the effectiveness of these measures.14 Such dialogue is almost nonexistent in Israel. The Comptroller’s Report is the exception that indicates the rule, and even that document conceals more than it reveals. The State Comptroller indicated the complexity of defensive information warfare, and the need for a single body to coordinate the issue of securing information in the State’s various computerized services, on the basis of a system-wide perception.15 In any case, what we can learn from the report is that the State of Israel is by no means ready to handle the threat of information warfare.

One of the most common and effective means of protection is the use of encryption software. In the legal sphere, the threat of information warfare demands a reconsideration of the regulation of encryption products. Such products serve the State in securing the information in its possession, but may also serve hostile groups in achieving their aims. This issue emphasizes the questions that underlie the whole discussion: the balance between security needs and individual rights, the cost of

12 http://www.nipc.gov
13 http://www.ciao.gov
14 http://www.infowarrior.org/articles/2000-06.html
15 According to the State Comptroller, defensive information warfare is built on a number of different levels: deterrence, warning, protection, identification and prevention of future attack, response at the level that has been attacked, and response on the national level (preparation of the State to cope in the absence of available computer systems in the accepted form, and the response of the State to aggressive information warfare from the outside). Based on this definition, the Comptroller raises a number of fundamental questions that require a response: who and what to protect? From what and from whom? Who will do the defending? How to defend and “how much”? and how to respond? In view of the mutual dependence between service systems, it is not enough for each body to plan independently, as has been the case up till now. Instead, there is a need for an overall systemic view of planning. See http://www.mevaker.gov.il/docs/52a/rtf/1e.rtf (last checked: February 2002).
intervention in the marketplace, and, fundamentally, the applicability of traditional legal concepts to the on-line environment. This issue will be dealt with more fully in the next chapter.

Monitoring

Along with the possibility of hostile elements using the digital environment as a weapon (direct use), the internet also serves as a communications medium for hostile forces to maintain contact among themselves, as well as a means for collecting information (indirect use). The main problem is that the Internet isn’t designed only to serve the needs of terrorists: an electronic mail message sent by one terrorist to another doesn’t include the heading: “Warning! Terror Mail.” For this reason, monitoring terrorist activity, in order to nip it in the bud, may need to infringe upon the privacy of others, and, indirectly, freedom of speech.

An additional difficulty is caused by blurring of the distinction between cybercrime and cyberterrorism. The distinction between the two concepts is based on the aims of the criminal/terrorist: The first term generally relates to “regular” crime, while the second is more associated with activities designed to strike at the fabric of democratic life. Again, these are two ends of a spectrum. At one end of the spectrum we would place the teenager hacker “playing” with the Internet for enjoyment, yet at the same time causing enormous damage (virtual, financial and even physical). At the other end of the spectrum is the terrorist, who uses the Internet to help him cause loss of life and property, in order to promote his political goals. Between the two lie an infinite number of other situations.

Note that the lack of uniform terminology is not only a semantic problem: labeling something as terrorism, particularly on the part of “security” bodies, provides the

---

18 See the discussions from the Shefayim Conference (discussion with the participation of Dr. Yariv Zfati, Dr. Yuval Karniel, Dr. Michael Birnhaack).
19 Given this background, it is interesting to examine the international convention promoted by the European Union to assist in the fight against crime: the Convention on Cyber-Crime. See http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm.
authorities with greater freedom of action in terms of the willingness of the public and the courts to accept the violation of individual rights, more so than in the case of “regular” crime, even if the methods and countermeasures are the same in both cases. Or, in legal jargon, the distinction may have implications for the quality of constitutional balances applied.

The picture becomes more complicated, when we add the point of view of the authorities: in this context, we need to distinguish between defensive measures and offensive measures. Here too we find a continuum, not a dichotomy. Defensive measures can be divided schematically into those aimed at preventing attacks, mainly by preventing disclosure of data (“field security”) and intelligence gathering, and those aimed at defending against an attack by means of data protection. Offensive measures include the location and apprehension of attackers (enforcement) or direct strikes at them, as well as using computer networks as an offensive weapon.

The third chapter deals with the limitations that apply to the use of monitoring measures in the on-line environment for security purposes.

**The Propaganda Arena**

Security threats associated with the on-line environment can also be classified based on the type of damage caused: physical or non-physical. In the framework of the latter category, we can include the term “SoftWar,” related mainly to the dissemination of false information for propaganda purposes, demoralization and so on. The legal problems that arise in connection with these issues of incitement, sedition, disinformation, hostile propaganda, and hate speech, have been dealt with in depth in the pre-digital environment. In that framework, at least in Israeli law, a series of constitutional balances was established to guide both the executive branch and the courts. The problems involve, for example, the tension between security needs and freedom of the press, the public interest in maintenance of order versus the freedom to demonstrate, and the limits on forms of political expression that offend the majority.

---

In principle, the questions that arise in the on-line environment are similar. However, the application of the existing balances in the digital environment, and the formulation of specific legal principles, requires discussion of the unique technological characteristics of the medium. This will be the topic of the fourth chapter. In particular, we will focus on the question of the responsibilities and liabilities of service providers.

A. The Problem

This chapter deals with the issue of regulation of encryption products. Encryption programs permit reasonable strong protection for data stored in digital networks, and are therefore relevant to security concerns in two ways, which, to a certain extent, are opposites. The first is the need to protect data held by defense and security bodies, as well as essential civilian systems such as hospitals, transportation services, food supplies, and communications networks (collectively, protection needs). The second need is that of retaining the technological ability to obtain information of defense value held by the enemy (monitoring needs). Protection needs pull in the direction of encouraging a software market without state interference, while monitoring needs pull in the direction of imposing limitations on the software market. In addition, intervention in the marketplace itself creates additional problems: changes in the incentive structure for research and development within the software market, violation of freedom of occupation and property rights, and a restriction on the ability of citizens to communicate securely and in privacy. This, in turn, impacts (indirectly) on freedom of speech.

In the past, a number of countries, including Israel, have imposed quite strict systems of regulation. However, over the years, these restrictive policies have been replaced by more moderate supervisory policies. This chapter will examine encryption, in light of the general considerations outlined above, and in light of the general trend toward liberalization. This is where technology raises security concerns, and, at the same time, creates interesting technological possibilities.

---

21 In preparing this chapter we were greatly assisted by lectures given by Dr. Gadi Aharoni, Adv. Mati Barzam, Prof. Martin Golumbic, Yoram Cohen, Dr. Ariel Sobelman, Prof. Eyal Kushilevitz, Prof. Hugo Krawczyk, Adv. Ram Raviv, Adv. Haim Ravia, and Yosi Shani, and to them we offer our thanks. Responsibility for the content, of course, is all our own.

22 See, for example, the Bezeq Law, 5742-1982, which states in Section 13(b)(3) that the Minister of communication is authorized to instruct a licensee, inter alia, in respect of carrying out the instructions of the General Security Service or the Israel Police, regarding the security classification of certain position-holders who are exposed to classified material, or those who have certain tasks, or regarding the maintenance of secrecy, protection of data or the protection of equipment and facilities on the licensee’s premises.
The discussion will begin with an overview of the technology, with an emphasis on its “natural” limitations. We will then examine security needs and existing legal frameworks. We will review the types of regulation adopted in the past in the United States and Israel, as well as key international arrangements, and we will look at the developments that have taken place in regulation policy. Following that, we will look at the implications of encryption policy, and the factors that need to be considered in formulating and applying that policy. These include various types of considerations. Some relate to the economic significance of regulation – intervention in the marketplace, the influence on incentives for software developers, and the influence on on-line commerce. Others involve human rights: freedom of occupation, property rights, and questions of privacy and freedom of speech.

In our view, a wise policy should strive to fulfill both kinds of security needs (protection and monitoring), while attempting to minimize intervention in the free market and limit the violation of human rights. Accordingly, we will indicate a number of possible legal models for dealing with this issue, which may serve as the basis for formulating a more intelligent policy in this area.

B. What is Encryption? The Technological Basis

1. Preface

Encryption has a long and interesting history. The theory of encryption was known by the Greek term, cryptography (“secret writing”). The use of encryption permits secret communication between two parties by means of a change – some sort of manipulation – of the information being transmitted. The two parties need to agree on the type of change and its details, in order to ensure the successful transmission of messages.  

---

Within defense frameworks, verbal messages of various types are transmitted – battle orders, intelligence data obtained from the enemy, and other messages that can be expressed in textual form. Traditionally, these texts were handed to encryption clerks, who were responsible for their encryption and transmission. The original text would be translated manually using some mathematical function – the key. The encrypted result would be transmitted, usually by radio or by courier. The working assumption was that the enemy might be able to put his hands on the encrypted text, but, as long as he didn’t have the key, the encrypted text was effectively immune to interpretation.

Deciphering of messages can be carried out with varying levels of activity on the part of the enemy – the listener. When all that the enemy can do is listen to the “live” transmissions, this is referred to as passive listening. If the enemy can also record messages and recreate them later on, this is active listening. The most active level is when the enemy has the ability to interpolate messages of his own into the communications stream, or to modify messages before they reach their destination. The tactical advantage that this offers is obvious.

The most secret element is, of course, the key – and its length is of critical importance here. Let us compare the key used for encryption to a simple combination lock. In order to open the lock one needs to select numbers in a certain order. If the key has a length of two digits, then there are 100 possibilities. Three digits – 1000 possibilities. Six digits – a million possibilities. The way to crack the lock would be to try to guess the combination, either at random, or by some systematic approach, a method called “Brute-Force Attack.” The longer the key, the more effort involved in cracking the code – and thus the quality of security will be better. The effort increases exponentially with the length of the key, and so a key of 64 to 256 bits is considered a sufficiently secure standard for most requirements. Also, note that a single letter of text is generally represented by 8 bits, in the commonly-used ASCII code, or by 16 bits in Unicode. Encryption of texts permits letters and symbols to be treated uniformly, and so, when we refer to a “letter”, we mean a letter or symbol.

---

25 In advanced computer environments, the Unicode system is used, in which each letter is represented by 16 bits (this allows 65536 possible characters). This method allows the encoding of characters from...
2. The Basic Principle of Encryption: Letter Replacement

One of the fundamentals of encryption is that of substitution: every letter is replaced by a different letter. This method was developed by Julius Caesar in his war against the city of Carthage. The key here was a string of 26 letters, related to the complete alphabet. The number of possibilities for the key is 26! (26-factorial, a number approximately equal to a 1 followed by 26 zeroes). If a computer calculates one result every microsecond, attempting to determine whether it has found the combination that will open the lock (that is, it carries out a brute force attack), the code breaking operation will last, on average, \(10^{13}\) years.

In spite of this, this approach is considered relatively simple to break, because of the statistical characteristics of the letters: the frequency of certain letters – e, t, a, o, i, n; the frequency of certain letter pairs, such as th, in, er, re, an; and so on. Thus, one can assign the letter with the highest frequency in the encrypted text to the letter “e”, and the second most frequent letter to the letter “t”, and so on, and then try to crack the key based on pairs and triplets.

3. Symmetrical Encryption

In spite of its shortcomings, the substitution method forms the basis for the first important digital encryption method, DES (Digital Encryption Standard), originally developed by IBM, under the name “Lucifer,” in the early 1970s, and adopted by the American government in 1977. The idea was to transform 64-bit blocks of source text into 64-bit blocks of encrypted text, using a series of mathematical steps based on letter substitution with a 56-bit key.

When a particular block of text appears twice in the message, it will be translated into exactly the same block of encrypted text. For example, if the 64-bit word “Example1” appears twice in the text, the encrypted translation will be identical in both cases. This consistency is, in fact, the characteristic that can be exploited to crack DES, similar to the statistical method for cracking letter substitution codes.


The DES method derives from the “Lucifer” system. “Lucifer” operated with 128-bit keys, but the United States National Security Agency (NSA) reduced the length of the key to 56 bits and demanded that the exact algorithm be kept a secret, so that the Agency itself could decipher messages encrypted by this method, while no other agency (with the limited computing resources available at the time) could do so. The high point of this policy was the NSA’s cancellation of cryptography conferences organized by the IEEE (the American Institute of Electrical and Electronic Engineers). The NSA issued legal orders, made threats and carried out monitoring to have the conferences cancelled, because of a fear that certain secrets might be revealed.

In 1977, two researchers at Stanford University, Whitfield Diffie and Martin Hellman developed a model for a machine that could break DES, and estimated that such a machine could be constructed at a cost of $20 million. Today, such a machine would cost no more than one million dollars. Such a machine would compare a passage of regular text with a passage of encrypted text, and would “run” possibilities until it had found the key.

In the early 1990s, two Swiss researchers, Xuejia Lai and James Massey, developed an encryption system similar to DES, but working with a key length of 128 bits. The system was named: IDEA – International Data Encryption Algorithm. Today, the patent for IDEA is held by Ascom Systems AG. At present, IDEA is considered unbreakable. Another, similar, method is called RC2/RC4. All of these methods work on similar principles, and are in general use throughout the world. These methods are called “symmetrical encryption” methods, since the two parties using the method use exactly the same key. They are also called “conventional encryption” methods.

27 The NSA has had reciprocal relationships with the world of encryption. In many cases, instead of a patent being registered for a certain invention or development, it has been requisitioned for the benefit of the Agency. For instances such as this, and others, see Kahn’s book (note 24 above), pages 672-736.
28 The method was issued U.S. Patent #3,962,539 (8 June 1976).
The weakness in symmetrical encryption

The weak link in all of the methods that we have discussed up till now is this: no matter how good the system is, if the enemy can steal the key, it will become useless. Since the key for encryption and the key for decryption are the same, there exists a problem: on the one hand we want to protect the key from being stolen, yet, on the other hand, it needs to be transmitted to all parties who need it, and so it can’t be kept totally secret. Since most encryption on the Internet still uses these methods, both parties need to agree, prior to communicating, on the encryption method and on the symmetrical key that they have chosen. It is clear that the first step, transmitting the key, cannot be secured by using the key – since the key has not yet been agreed upon.

4. Asymmetrical Encryption: Public Key and Private Key

Here the RSA method enters the picture. Named after its three developers, Rivest, Shamir and Adleman, this method doesn’t work on the principle of symmetrical encryption, but on the principle of a public key, a fairly modern addition to the concepts of cryptography (that is, over the past thirty years). In this method, every user has two keys, a public key – which is used by the “rest of the world” to send messages to the user, and a private key, utilized by the user to decipher the messages sent to him. The popular home encryption program PGP (Pretty Good Privacy)\(^\text{32}\) applies this method in an easy-to-use way. RSA is used for the initial transmission of keys for that session, and then DES or IDEA, which are much faster methods, can be used.

Analysis of the RSA method

Now we will attempt to demonstrate the mathematical basis for the RSA method.\(^\text{33}\) For this purpose, it is important to understand some simple fundamental concepts:

**Computational Problem** – A problem that accepts a certain input and calculates a certain output (the solution to the problem).

There are two types of such problems:

\(^{32}\) The program was developed by Phillip Zimmerman. A practical instruction book that describes how to get the most out of it is: Simson L. Garfinkel, *PGP: Pretty Good Privacy* (1995). The book also describes the history of the program, and the problems faced by its developer (pp. 85-116).

A problem is **tractable** if a method is known to solve it, that is, if there exists a fixed method, or algorithm, that can handle all possible inputs to the problem, and solve it in a predictable (relatively short) amount of time.

A problem is **intractable** if no known general solution exists that can solve the problem in a *controlled amount of time*. As we shall see, intractable problems can be utilized to create secure keys, and transmit data through public communications channels, as happens in RSA.

The general idea is, that those sending messages to each other hold additional information that will help solve the (specific) intractable problem immediately, while someone trying to crack the encrypted data (without the additional information) will encounter a problem that can only be solved by attacking it with supercomputers running for hundreds of millions of years (something that, of course, is practically impossible). That is, for the parties to the communication, the problem is tractable, while for someone who is not a party to it, the problem is intractable.

In the RSA system, which was first presented in a scientific journal in the United States in 1977, there are three loci of information: the **sender** of the message, the **receiver** of the message, and the **public domain** (for example: the advertising section in a newspaper, or a non-encrypted area of the internet). We will now demonstrate how the system operates in practice. This is the method that was protected by a patent that expired in September 2000.35

These are the items of information involved in the process:

\[
p, q = \text{two prime numbers, selected by the recipient and not given to anyone else (even the sender). The recipient can select them by means of a random prime number generator, since the test to determine whether a number is prime is a tractable problem, as compared to finding the factors of a number, which is intractable.}^{36}
\]

---

35 U.S. Patent #4,405,829.
n = p * q – placed by the sender in the **public domain**.

t = (p-1)*(q-1), calculated by the **recipient** and not given to anyone else (even the sender). This will afterwards be used to generate the private key.

E – some number whose highest common factor with t is 1 (in other words, it is relatively prime to t). This number can be easily calculated by the **recipient** (since t is known to him), and this number is also placed in the public domain. That is, n and E are a pair of public keys.

M – the message that the **sender** would like to send. Again, it is easier to consider the message as a string of binary bits (0, 1). If we treat it as a single binary number, its decimal value will be M. (The sender needs to check first that M is less than n.)

D – in addition to all of these, there is another piece of information calculated by the **recipient**, and that is the multiplicative inverse of E, modulo t, that is: D*E = 1 (mod t). Since t is known to the recipient, he can easily calculate D. The modulo operation gives the remainder after dividing by t. The recipient keeps D secret, and does not pass it on to anyone.

**So far we have the following**: The recipient has D, t, p, q. The sender knows M, and everybody knows n and E.
In particular, D is the recipient’s private key (which will serve to decipher the message), E and n are his pair of public keys (which will be used by the sender to encrypt the message to be sent to him).

To send the message: The **sender** takes the message M, checks the public keys n and E, calculates the encrypted message C and sends it through an open (unprotected) communications channel. C can be calculated mathematically as follows: $C = M^E \pmod{n}$, where $^E$ stands for “raised to the power of”.

It is easy to see that the sender does not have his own codes, and in fact has nothing secret other than the message M itself; the encryption process itself is immediate.

In order to decipher the message: The recipient receives C, and can immediately extract the original message M, as long as he still has his private key D: $M = C^D \pmod{n}$.

**Example:**

The recipient selects two prime numbers p, q: 2, 5, and calculates n: 10, which he publishes in the public domain. Of course, for practical purposes, the recipient needs to select values of p and q that are much larger (so that the enemy cannot easily factorize n, the characteristic on which RSA is based).38

The recipient calculates t: $t = (q-1)(p-1) = (5-1)(2-1) = 4 \times 1 = 4$.

The recipient also calculates E: He looks for a number that is relatively prime to t, that is, relatively prime to 4. If he chooses the number 3, this would appear to be suitable, since 3 and 4 are relatively prime (that is, their highest common factor is 1 – which meets the definition’s criteria). If he would have picked $E = 2$, this would not work, since the highest

---

common factor of 2 and 4 is 2 (does not fit the definition, which requires the highest common factor to be 1).

As we have said, the recipient places these two (the public keys) in the public domain: \( E = 3, n = 10 \).

The recipient now calculates \( D \): This is the multiplicative inverse of \( E \), modulo \( t \), that is \( D \times E = 1 \mod t \). Since \( t \) is known to the recipient, he can easily calculate \( D \):

\[
D \times E = 1 \mod t \\
D \times 3 = 1 \mod 4 \\
9 = 1 \mod 4 \\
D = 3
\]

\( D \) is the recipient’s private key, and he keeps its value (3) secret.

Now, let us suppose that the original message, after conversion to bits is \( M = 7 \). This is the message that the sender wants to send to the recipient (obviously, in practical applications, the numbers are very much larger).

The sender calculates the encrypted message \( C \) by substitution in the formula: \( C = M \times E \mod n \)

\[
C = M \times E \mod n = 7 \times 3 \mod 10 = 343 \mod 10 = 3
\]

Note that the sender uses both public keys \( n, E \) to turn the original message \( M \) into the encrypted message \( C = 3 \).

Now that the recipient has received the encrypted message 3 – let us see how he recreates the original message using the private key in his possession, \( D = 3 \):

\[
M = C \times D \mod n = 3 \times 3 \mod 10 = 27 \mod 10 = 7
\]

The enemy has no way of knowing that the encrypted message \( C = 3 \) is in fact the encryption of \( M = 7 \), since he doesn’t know the private key \( D \) (which derives from \( p, q \), the factors of \( n \)). The decryption is complete.

The RSA method is based on the mathematical characteristic that the problem of breaking a large number into its factors is an intractable one. What does this mean? At
a mathematical convention held in 1903, one of the speakers declared that the large number $2^{67} - 1$ was not prime, and, to convince his listeners, all he had to do was write: $2^{67} - 1 = 193707721 \times 761838257287$. It is obvious that the speaker had to work very hard to find those factors, but, the moment he found them, it was easy to prove his contention that their product is not prime. The problem is, of course, to factorize large numbers such as $2^{67} - 1$, when one knows nothing about where their factors might lie.

At present, whole numbers of up to 200 digits can be factorized within hours using a very powerful computer. However, if we consider a page of text, about the length of a printed page, then such a message can contain about 8000 bits\textsuperscript{39} which translates to a decimal number with 2400 digits,\textsuperscript{40} significantly larger than the 200 digits that can be handled at present. Thus, an encrypted message of about a page in length is located far into the “field of intractable problems,” and thus, unlike DES, it is impossible to break RSA.

The security provided by the RSA system is dependent to a large extent on the difficulty of factorizing large whole numbers. If the enemy can factorize the number $n$ into its factors $p$, $q$, then he should be able to decipher the message. If we randomly select two prime numbers, each 150 digits in length, and multiply them together, we can create a public key $n$, 300 digits in length, that cannot be cracked within a reasonable time using the technologies available at present. Without a significant breakthrough in developing number theory algorithms, the RSA encryption system will still provide the highest level of security in the world of encryption.

C. Security Needs

The security needs in this topic can be divided into two main goals: data protection needs and monitoring needs. Apart from these two needs, and in light of the fact that strong encryption products are readily available on the open market, we need to

\textsuperscript{39} A page of text contains approximately 1000 characters, which is 8000 bits (in the commonly used encoding system, ASCII, each letter is represented by 8 bits).

\textsuperscript{40} $2$ to the power of 8000 is $10$ to the power of 2400.
explain the main motive for regulation: the desire to make it harder for the enemy, and this includes terrorist organizations.

1. Data Protection

Essential government systems, as well as essential civilian systems, require maximal protection. Penetration of these systems can cause damage of various types: beginning from damage to the computer systems themselves, thus causing mainly economic damage, through the theft of data and its misuse, up to the disruption of these systems’ activities in ways that will cause physical damage in the real world. These actions are various aspects of cyberterrorism. Thus, for example, it is possible to “destroy” key financial systems in the economy, or to paralyze the supply of electricity in the State. Cyberterrorism of this type requires significant computational power, in order to crack complex codes that serve to protect information systems. The dissemination of supercomputers, capable of carrying out computations of this nature, is limited. The aim is to prevent terrorists from accessing sensitive data.

We should note at this juncture that, since defense and security bodies develop their own encryption products they are the owners of the products and the knowledge, and there is no difficulty in limiting the dissemination of these encryption products. However, this fact alone is insufficient to justify the regulation of encryption products that were developed in the free market, outside the defense establishment.

It has been claimed, at least in Israel, that many leading industry figures come out of the defense establishment, and that there exists a fear of information drift. We would like to point out that, even if this is true, it would still not, on its own, justify the regulation of encryption products. The way to deal with this understandable concern about information drift is by means of restrictive contractual provisions, proprietary protections (trade secrets) and criminal sanctions (prohibitions

42 Shelach, ibid.
relating to spying, etc.), but not through direct intervention in the encryption market.\textsuperscript{43}

It is also worth mentioning that demand for data protection exists within the civilian market as well, and, at times, data protection is required by law. Thus, for example, the \textbf{Patients’ Rights Law}, 5756-1996 requires a person providing treatment or an employee of a medical institution to keep information about patients secret. It also requires the directors of medical institutions to adopt protective mechanisms for this purpose.\textsuperscript{44} The \textbf{Privacy Protection Law}, 5741-1981, imposes on the owner, holder or manager of a database, as well as on certain public bodies, banks, insurance companies and other financial bodies, an obligation to protect the data in their possession.\textsuperscript{45}

\section*{2. Monitoring – Intelligence}
The first practical means of defense against terrorism is intelligence.\textsuperscript{46} In order to thwart terrorist activity, defense and security agencies need to obtain good intelligence, including data on terrorist intentions and information on their daily moves.\textsuperscript{47} Therefore, security agencies need the ability to decipher encrypted transmissions. A fundamental assertion (which had a certain validity when the Encryption Order was first issued in 1974) states that limitations on and regulation of encryption technology in general, and not granting permits for the use of reasonably “strong” encryption in particular, would keep such technology out of the hands of those whom the intelligence services were targeting; an orderly system of registration and licensing would also provide a certain amount of information about and control over the uses of encryption.

\begin{itemize}
\item[\textsuperscript{43}] See Parts 4 and 5 of chapter 7 of the Israeli Penal Code, 5737-1977.
\item[\textsuperscript{44}] See Section 19 of the \textbf{Patients’ Rights Law}, 5756-1996, \textit{Sefer Hukkim} 330.
\item[\textsuperscript{45}] See Section 17 of the \textbf{Privacy Protection Law}, 5741-1981, \textit{Sefer Hukkim} 128. For a critique of the scope of this obligation, see Avi Zilberfeld, “\textit{Hok Haganat HaPratiut – Hashlachot Ma’asiyot} [The Privacy Protection Law – Practical Implications], \textit{Machshevim PC} 1987, 8-10.
\item[\textsuperscript{47}] Kupperman and Trent, ibid, p. 147 (Hebrew edition).
\end{itemize}
In the past, security forces throughout the world have come up against attempts by terrorist organizations and other hostile elements to conceal their activities by means of encryption. Thus, for example, a statement by the director of the FBI before the Senate Select Committee on Intelligence\(^{48}\) noted the use of encryption by the spy, Aldrich Ames, who was asked by his Soviet handlers to encrypt the material he transmitted to them. Similarly, the plot by Ramzi Yousef and other terrorists, to blow up eleven American airliners in the Far East was also mentioned. Yousef’s portable computer, which was captured in Manila, contained encrypted files relating to the terrorist plot.

Intelligence is a complex art, and the volume of communications passing through modern communications channels has become a challenge for intelligence agencies with limited resources. It is therefore necessary to map information flows and focus on intercepting the most important channels. This will allow intelligence services to concentrate their closest attention on the most important messages, out of the total volume of messages passing through the various channels. It is only after this stage that the more familiar part of the intelligence process takes place. For this purpose, the message has to be stripped of its protective mechanisms (this generally means encryption) before any intelligence assessment of its nature and content can take place. Those who think in terms of the vulnerability of communication from a security point of view see encryption as intelligence’s main obstacle. In addition, an enemy who is aware of the way in which his communications are being used may try to modify these channels in order to make their utilization more difficult.\(^{49}\) Encryption is one of the most effective means of achieving that goal.

Therefore, the greater the restriction on the use of encryption and the ability to market sophisticated encryption products, the easier it will be for security agencies to intercept transmissions containing information that can lead to the prevention of terrorist acts. Conversely, the more access that terrorists have to unbreakable encryptions and the technologies to create such codes, the more difficult it would be to prevent such terrorist acts will become.


3. The Rationale for Regulation

In spite of these security needs, it appears at first glance that technology has already won. Encryption technology exists on the open market, and is available to anyone who wants it: in shops and on the Internet, either at a reasonable price or for free. In view of the fact that today national borders no longer pose any real obstacle, and particularly in view of the fact that the digital environment can easily hurdle such obstacles, the question then arises: is there indeed any justification for regulation?

It appears that the answer is “yes”, for two reasons. The first is a moral reason, and the second is a practical reason. The moral reason is that, even if encryption products are available to terrorists, this does not justify making things easier for them. In other words, the fact that enforcement, in the sense of totally controlling the distribution of encryption products and preventing terrorists from acquiring them, is difficult – even to the point of failure – does not justify giving up.\(^{50}\)

The practical reason is two-fold. Firstly, in dealing with terrorism, it is important for security agencies to know what technology the terrorists use, if at all. Such information will make it easier for states to plan to thwart terrorism. In addition, where the state has a “back door”, that is, a ‘super-key’ that allows it to penetrate beyond the encryption, its access to terrorist information will be greatly increased. Secondly, in order to utilize an encryption product in the most efficient manner, technical support from the developer is usually necessary. The more a developer is restricted, the harder it will be for a terrorist to use that particular encryption product.

Therefore, we believe that security considerations exist and are valid, in spite of the easy availability of strong encryption products on the open market. At the same time, security considerations need to be balanced against other considerations. These will be examined in section E, but before we do so, we would like to review existing legal frameworks and the changes that have taken place within them in recent years.

\(^{50}\) For an argument in a similar vein, see: Codes, Keys and Conflicts, ibid.
D. The Legal Framework

This section will present the current legal framework for regulation of commercial encryption products, firstly as it pertains to Israel, and then in the broader international context, in the United States and Britain. Additional legal arrangements apply to encryption products developed by the military, but these add no real difficulties, and it is clear that the military has both the (proprietary) right and (governmental) authority to limit their drift into the private market.

1. Israel: From Blanket Prohibition to Prior Licensing and Subsequent Control

The basis for the legal regulation of encryption in Israel is in secondary legislation, by virtue of the Control of Products and Services Law, 5718-1957 (hereinafter: the empowering law).\(^{51}\) By authority of this law, the Defense Minister, in 1974, issued the Control of Commodities and Services (Engagement in Means of Encryption) Order, 5734-1974,\(^ {52}\) and the Control of Commodities and Services (Engagement in Means of Encryption) Declaration, 5734-1974.\(^ {53}\) The arrangements established in these regulations required a person to obtain a license before having involvement in the means of encryption. In 1998, a significant amendment was applied to the existing arrangement. This change meant that Israel passed from a regime that imposed a blanket prohibition on any involvement in encryption methods without a prior license, to a more liberal regime, which established a policy of more limited control. The change is expressed in the determination that certain dealings in encryption were now permitted occupations, that did not require any license, and in the establishment of three levels of license for other involvement in the means of encryption.\(^ {54}\) There does exist, however, a significant gap between the legal authority granted under the law

---


\(^{52}\) Control of Commodities and Services (Engagement in Means of Encryption) Order, 5734-1974, *Kovetz Takanot* 5735, 45 (the Encryption Order).

\(^{53}\) Control of Commodities and Services (Engagement in Means of Encryption) Declaration, 5734-1974, *Kovetz Takanot* 5735, 46 (the Declaration).

\(^{54}\) Sections 1(3) and 3 of the Control of Commodities and Services (Engagement in Means of Encryption) (Amendment) Order, 5748-1998, *Kovetz Takanot* 5748, p. 1107 (the amended Encryption Order).
regarding the licensing of encryption, and the policy adopted in practice, which is much more moderate.55

In this subsection we will first outline the Control of Products and Services Law, 5718-1957, under which the subordinate legislation was issued. We will then discuss the arrangements established by that subordinate legislation, and afterwards discuss the significant changes in the legal arrangements regarding encryption since 1998, the policy adopted in practice, and the differences between them.

The framework of the legal arrangements up to 1998

The application of the empowering law, under which the subordinate legislation regulating encryption was promulgated, is dependent on the existence of a state of emergency in the country.56 This law is a framework law, granting the minister or any member of the government,57 broad authority to regulate, by order, the production, sale, consumption, use, and so on, of a product or service,58 provided only that he has reason to believe that this is necessary to maintain an essential activity, prevent speculation or prevent the public from being defrauded.59 The legislative history teaches us, the aim of the law is to assist the government in regulating the country’s economy in times of emergency and in ensuring the economy’s development and growth, while protecting the citizen from inequity. In emergency situations, this usually takes the form of black marketeering, speculation, hoarding, or price increases.60 In light of this aim, the question arises whether the regulation of encryption, which is a security issue, should be carried out under this law.61 Although “essential activity,” which justifies the minister’s intervention, includes action to

---

56 Section 2 of the empowering law. In the past, a state of emergency was declared under Section 99a) of the Law and Order Ordinance, 5708-1948, and currently under Section 49 of the Basic Law: The Government. The state of emergency has never been cancelled.
57 In accordance with the definition of “Minister” in Section 1 of the empowering law.
58 Section 5 of the empowering law.
59 Section 3 of the empowering law.
60 Divrei HaKnesset 21 (5717) 103-105.
61 See, for example, Barukh Beracha, Mishpat Minhali [Administrative Law] (Volume 1 5747) 87-88. The author criticizes the broad powers given to ministers to issue regulations under the Control of Products and Services Law, in the absence of substantial parliamentary review. In the author’s view, the state of emergency has sometimes served as cover for use of the legislative authority under the Control of Products and Services Law, without any connection to the actual existence of a state of emergency.
protect the security of the State and the public, the intention of the legislator was to provide the tools for dealing with the economic situation in a state of emergency. Therefore, it may be argued that, in light of the principles of administrative law, we have here an overstepping of authority.

In our opinion, the fact that these Orders go beyond the authority provided in the law is a prime reason for having the issue covered by a separate, direct legal arrangement, explicitly provided for in primary legislation, and not hidden under the camouflage of economic legislation.

In this we concur with the recommendations of the Knesset’s Subcommittee on Israel’s Preparedness for the Information Age, to enact a law that regulates the authority and overall responsibility for control of the means of encryption and licensing the engagement in them.

The broad authority granted to the Minister to issue Orders under the empowering law is subject to judicial review. In the Knesset debate when the law was adopted, it was proposed that a parliamentary review mechanism be set up in addition to the judicial review. According to that proposal, Orders that have legislative effect would be brought for the approval of the Knesset’s Finance Committee, and the latter would be entitled, where it saw fit, to request the Knesset to repeal such orders. This proposal

---

62 “Essential activity” is defined broadly, in Section 1 of the empowering law, as “an activity which appears to the Minister to be essential for protection of the State, for public security, to maintain orderly supply of goods or services, to establish stability in the prices of commodities or the fees for services, to increase exports, to absorb immigrants or for the rehabilitation of discharged soldiers or war disabled.”

63 As can be seen from the statement by the Knesset Finance Committee chairman, MK Binyamin Avniel, when he presented the law before the Knesset plenum for its second reading. Divrei HaKnesset 23 (5718) 421.

64 The Subcommittee on Israel’s Preparedness for the Information Age was established in 1997, in the framework of the Knesset Committee on Information and Computer Systems. It should be emphasized that the committee’s report was published prior to the changes in the Encryption Order in 1998 (the Subcommittee for Information and Computer Technology).

65 Amnon Rubinstein, Barak Medinah, HaMishpat HaConstitutzionali shel Medinat Yisrael [The Constitutional Law of the State of Israel] (Volume 2, 5th Edition, 5747), 812-833, 1165-1170. Judicial review examines the Minister’s discretion in issuing the Orders in general, whether the minister used the authority for one of the purposes defined in Section 3 of the empowering law, and whether the aim of the Order is related to the existence of a state of emergency. In the authors’ view, the trend toward applying judicial review to the use of emergency powers under the empowering law, will increase after enactment of the Basic Law: Freedom of Occupation. Regarding the violation of freedom of occupation, see below, section E.5 of this chapter.

66 Divrei HaKnesset (5718) 421-422, statement of MK Binyamin Avniel.
was not accepted, and so the only review mechanism that exists in respect of the Minister’s authority to issue Orders is judicial review.\(^67\)

**Regulation of this issue in primary legislation is also appropriate, therefore, in light of the principle of separation of powers, and in order to provide effective review of the actions of the executive branch.**

By virtue of Sections 4, 5, 15 and 43 of the empowering law, the Defense Minister enacted, in 1974, secondary legislation dealing with the issue of encryption: the Control of Commodities and Services (Engagement in Means of Encryption) Order, 5734-1974, and the Control of Commodities and Services (Engagement in Means of Encryption) Declaration, 5734-1974. The empowering law establishes the policy principles and basic parameters. The Order and Declaration are subordinate legislation that the executive branch is empowered to enact by virtue of specific authority granted under the law.\(^68\) In general, the executive branch has the authority to establish secondary arrangements, but in practice the legislature also hands over the authority to enact primary arrangements. Regulations of this nature are called *prater legem* (“outside the law”) regulations, since they not only establish the provisions to carry out the arrangement established in the law, but also additional provisions, which establish arrangements and principles beyond those established in the law. In such cases, the primary legislator is content to set the goals, the achievement of which requires subordinate legislation. The bulk of economic legislation is of this type, and it gives the secondary legislator a great deal more freedom of action. The Control of Commodities and Services Law empowers the Minister to establish, by means of Orders, extensive economic controls. The law details the means of control and the aims for which the authority may be used, but it does not determine any arrangement regarding the content of such control.\(^69\) So too in our case: The Encryption Order applies the provisions to be implemented regarding the licensing of engagement in the

---

\(^67\) *Divrei HaKnesset* (5718) 429-430.

\(^68\) Section 1 of the Interpretation Ordinance [New Version], which is the definitions section, includes, *inter alia*, under the term “Takanah” [Regulation] both Order and Declaration. An Order and a Declaration are different types of regulation, which the executive branch may issue as subordinate legislation. The difference between an Order and a Declaration is that an Order applies specific provisions for implementation of general provisions found in the law, while a Declaration has a declarative nature – it informs or announces, but does not contain provisions for implementation.

\(^69\) See Rubinstein and Medinah, supra note 65, at 803.
means of encryption, while the **Declaration** gives notice of those products that are subject to control: data, means of encryption, encryption methods, encryption keys, records relating to encryption, and the engagement in means of encryption.

**In our opinion, it is inappropriate to place the policy making in the hands of the secondary legislator. The existing system of regulation regarding encryption is primary in nature, and it is appropriate that it should be established by the legislature. This is an additional reason for regulating the issue through primary legislation.**

**Nature of the Arrangement**

It appears that the Encryption Order was aimed at providing a balance between the need to protect the national security of the State of Israel on the one hand, and the desire to allow reasonable competition within the Israeli encryption market, without imposing restrictions that were too onerous on producers and users, on the other hand.\(^{70}\) The key principle established in the Encryption Order is that of conditioning the engagement in means of encryption on obtaining a prior license.\(^{71}\) The authority to grant permits and licenses is vested in a “Director” appointed by the Minister of Defense. In practice, the Director-General of the Ministry of Defense was appointed to this position, and the latter delegated his authority to the Supervisor of Military Export Controls.\(^{72}\)

The Director has the authority to enter any place where engagement in means of encryption takes place, examine the means of encryption, and request additional details from the license applicant, both prior to deciding on the license application, and after the license is granted.\(^{73}\) The Director has extensive authority regarding the

\(^{70}\) As stated in Section 1 of the Ministry of Defense Policy, see supra note 55.

\(^{71}\) See Section 2(a) of the Encryption Order. Engagement in means of encryption is defined in Section 1 of the Declaration in the broadest terms, including development, production, possession, use, import, export, transport, transfer, distribution, sale or acquisition of means of encryption, encryption methods or encryption keys.

\(^{72}\) Section 1 of the Encryption Order. Until the amendment in 1998, the Director was the IDF Chief Communications, Electronics and Computers Officer. See the Ministry of Defense website: http://www.defence.gov.il/modh1/encryption/index.html

\(^{73}\) Section 6 of the Encryption Order.
grant of a license, and, as a result, has broad discretionary powers in this connection.\(^{74}\)

Of course, the way in which this authority is used by the Director, and his decisions, are subject to judicial review on grounds of administrative law.\(^{75}\) Among these we should note in particular the grounds of reasonableness and proportionality, and subordination to the Basic Laws.

**The Changes in the Legal Arrangements**

In light of technological developments and the increasing criticism of the sweeping limitations imposed by the Encryption Order and Declaration,\(^{76}\) a significant change was made in 1998 in the subordinate legislation applying to encryption. This change was brought about by the issue of the Control of Commodities and Services (Engagement in Means of Encryption) (Amendment) Order, 5748-1998,\(^{77}\) and the Control of Commodities and Services (Engagement in Means of Encryption) (Amendment) Declaration, 5748-1998.\(^{78}\)

Prior to this change came the report on Data Protection from the Knesset’s Subcommittee for Information and Computer Technology. The committee pointed to a number of difficulties in the then legal arrangements, which justified legislative and

---

\(^{74}\) Section 5 of the Encryption Order: “The Director is entitled to issue the license, refuse to issue it, establish conditions for its issuance, suspend or revoke it, as he sees fit.”

\(^{75}\) For the extent of judicial review on the use of powers by an administrative authority, see Rubinstein and Medinah, supra note, at pp. 347-359.

\(^{76}\) For further details, see Victor Bougnim, “Tashhit Mishpatit LeMishar Electoni [Legal Infrastructure for Electronic Commerce]”, *Sha’arei Mishpat*, 1 (5748), 169. The article was written prior to the change in the regulations in 1998. The author explains that the Encryption Order and Declaration are too broad in light of the technological realities of the time. Two areas where this was so were identified: the definition of means of encryption to which the controls were applied (at the time, the Order applied to all means of encryption, even the simplest) and the range of activities subject to control (the definition was so general that it could have been argued that even the study of Biblical encryption methods was subject to control). The author recommended that the legislation applying to encryption in Israel be amended to adapt it to the changing circumstances. See also Brian Nigan, Itzik Yarhi, “Skirah Mekutzeret – Kod HaTzofen [Brief Overview – The Encryption Code]” (1997), available at http://www.itpolicy.gov.il/vadat_inter.gov/articles/zofen.htm. This article, too, was written before the amendment of the Encryption Order and Declaration in 1998. The authors criticized the existing legal situation regarding encryption in Israel, and recommended that a scale of licenses be established for engagement in means of encryption: A general license for use of encryption measures for identification purposes, while ensuring that these measures cannot be modified to allow encryption of data, and establishment of a license to deal in data encryption measures, taking into account the balance between security considerations, commercial and internet reliability issues, and the individual’s freedom to protect his own privacy.


\(^{78}\) Control of Commodities and Services (Engagement in Means of Encryption) (Amendment) Declaration, 5748-1998, *Kovetz Takanot* 5748, p. 1109 (the amended Declaration).
governmental intervention. The committee noted that the Encryption Order remained in force mainly for security reasons, that is, the desire to keep sophisticated encryption technology in the hands of the security authorities. However, in light of the current availability of encryption technologies to anyone who wants them, this rationale had been weakened, and thus sweeping control of the various dealings in encryption measures was no longer appropriate.\textsuperscript{79} Therefore the committee recommended limiting restrictions on export of the means of encryption, and to leave them in place only in respect of countries defined as a security threat to Israel. The committee proposed that an Order establish significant relief in the form of a general license for various dealings in encryption measures, with the exception of defense activities.\textsuperscript{80} Not all of the committee’s recommendations regarding amendment of the Order were implemented. Below we will examine the main changes that were adopted.

The key changes that were adopted in 1998 are:

1. Transfer of the sole authority for control of means of encryption and the granting of licenses to engage in the means of encryption, to the Director-General of the Ministry of Defense.\textsuperscript{81}

\textsuperscript{79} The committee found that the Order, in its 1974 format, prohibited various uses of encryption measures, which, in fact, were freely available on the market. The Encryption Order created a situation in which citizens and organizations using those products were actually breaking the law, while others refrained from using existing measures, and thus were prevented from developing and competing in the global market. Regarding data protection, the report states that the Order limits the ability to use data protection measures and the development of governmental information systems. As for the development of electronic commerce, the committee pointed out that a literal application of the Encryption Order’s provisions did not allow the use of encryption technologies, their application or export.

\textsuperscript{80} The committee recommended a fundamental change in the legislation applying to the use of and dealings in encryption measures. This change was deemed essential in order to adapt the legal position in Israel to economic and commercial developments. Firstly, it was recommended to apply those criteria that applied to encryption products that were free of control or restrictions on their use and export. Secondly, it was recommended that amendments be made in the Encryption Order, which, in 1974, had applied sweeping definitions, restrictions on internal and external uses of encryption, and a bureaucratic procedure for obtaining a license. Thirdly, they recommended that a law be enacted to regulate the general authority and responsibilities for control of encryption measures. The committee also recommended the establishment of the Data Protection Authority, which would operate on the basis of making as much government information available to the public, while maintaining the security of governmental data systems. In addition, it was recommended that a supra-departmental body be set up to deal with threats to national data systems networks. The State Comptroller’s report No. 52a indicates that within the General Security Service there is a body called the “National Data Protection Authority.” The Ministry of Finance runs the Tehilah Project, which is one of the bodies involved in implementing data protection. Tehilah was established at the recommendation of the National Data Protection Authority, and operates under its direction.

\textsuperscript{81} Section 1(2) of the amended Encryption Order.
2. Empowerment of the Director to declare a means of encryption as a “free means”. A “free means” is a means of encryption that has been removed from the category of controlled items, and dealing in it does not require a license, or for which a general license has been granted.\textsuperscript{82}

3. The granting of an exemption from a license for any dealing in a free means of encryption, with the exception of development, production, modification and integration of a free means of encryption.\textsuperscript{83} In addition, the granting of an exemption for any purchase, use or possession of a means of encryption, if the sale or transfer of the means of encryption to the person concerned was carried out pursuant to a license from the Director-General.

4. The creation of a scale of licenses for dealing in the means of encryption, as opposed to the original Encryption Order and Declaration, which did not contain such a classification.\textsuperscript{84} The amending Order does not define the criteria for licensing the use of encryption measures.

\begin{table}[h]
\centering
\begin{tabular}{|l|}
\hline
\textbf{Scale of Licenses} \\
\hline
\textbf{General License} – given for all types of dealing in encryption measures, with the exceptions of modification and integration. \\
\textbf{Limited License} – given for certain types of encryption measures, to a certain encryption measure or destination country, based on criteria such as the type of user of the means of encryption. \\
\textbf{Special License} – given for certain dealings in a certain encryption measure. \\
\hline
\end{tabular}
\end{table}

5. The definition of “class of user” of means of encryption as “financial institution, government institution, or incorporated body, institution or organization of another kind authorized by the Director.” It appears that this specific definition of the type of user means a limitation in the control carried out under the Encryption Order. Unlike the general application of the

\textsuperscript{82} Section 3 of the amending order, which adds Section 3b to the Encryption Order. So, for example, the Director defined the internet browsers Internet Explorer and Netscape Navigator, and the programs Microsoft Office and Winzip, as free means. See: http://www.mod.gov.il/modh1/encryption/tzofend.htm.

\textsuperscript{83} Section 3 of the amending order, which adds Section 3a to the Encryption Order.

\textsuperscript{84} Section 1 of the amended Order.
Encryption Order to “any person engaging in the means of encryption,” control under the amended Encryption Order would now apply to a specified or defined group of users.

6. The Order provides for the establishment of an advisory committee, one of whose members will be a public representative, and which will be headed by the Supervisor of Military Export Controls.85 The committee’s task is to consider the applications for a license to engage in means of encryption. Where the committee recommends that the application be rejected, the Director will accept that recommendation, and notify the applicant of the decision, providing the reasons for that decision. The Director is also permitted to delegate his powers to the advisory committee, or to any subcommittee that the committee may appoint, with the exception of the power to grant, refuse to grant, rescind or condition any license.86 Moreover, the Order does not detail the licensing process.

7. Regarding the export of encryption products, the Order states that export permits will not be given in respect of a limited number of countries. As part of the policy of controlling engagement in commercial means of encryption within the territory of the State of Israel, the Order provides that the holder of a license to sell encryption means must obtain authorization prior to selling such means to the Palestinian Authority.

The amended Order is an important stage in liberalizing control over encryption, and this trend is in line with the current trend in the Western world. At the same time, there is a gap between the policy adopted in practice and the legal framework, in that the policy actually adopted is even more liberal than the legal authority. In our opinion, the present trend is desirable. However, the gap between practical policy and the broader legal authority has negative implications for research and development considerations in the industry.

Therefore, we believe that the trend toward liberalization ought to be continued, and it is in that spirit that the primary legal framework ought to be shaped.

86 Section 4 of the Amending Order, which adds Section 10a to the Encryption Order.
2. United States

In recent years, the legal regime applying to encryption in the United States underwent a fundamental change, with the trend to reducing restrictions and prior control. Regulation of encryption in the United States can be divided into two periods.

Up to 1996, the export of the means of encryption with a key length (strength) above 40 bits\(^\text{87}\) was considered as export of munitions, and the control of trade in encryption means was carried out through the ITAR – International Traffic in Arms Regulations. Since there were severe restrictions, and in order to respond to the needs of the software market, in 1993 the Administration proposed the idea of the Clipper Chip, which would be a means of encryption licensed by the Administration, with the Administration retaining the means to decipher the Clipper Chip. In this way, the Administration would retain the ability to access any content encrypted by means of this chip. The idea was not successful. Opposition came from software companies, which were restricted in terms of software exports and competitively disadvantaged in world markets, and from human rights organizations and privacy advocates.

In November 1996 the Administration changed its position, and the previous regime, of a sweeping prohibition with only limited exceptions, was replaced by a regime of export restrictions, from some of which exemptions could also be obtained.\(^\text{88}\) Encryption means were now only considered as munitions if they were for military purposes. The Administration’s goal was to support electronic commerce, to protect global information infrastructures, to protect privacy, intellectual property rights and important information, and to allow American companies to compete equally with their overseas counterparts. Authority for the control of encryption was transferred to the Bureau of Export Control (BXA), which is subject to the Department of Commerce. Encryption items were reclassified: they were transferred from the Munitions Control list to the Commerce Control list. The new regulations created a process by which the owner of means of encryption with a key length of up to 40 bits could have the product removed from the Commerce Control list after a single examination by the BXA, and then would be exempt, in practice, from any export.

\(^{87}\) For a technical explanation, see Section B of this chapter.

\(^{88}\) Executive Order 13026 (November 15, 1996).
Similarly, it was possible to obtain an export license, but not removal from control, for encryption items that operated with 56-bit keys using DES technology \(^{90}\) (or equivalent), subject to two conditions: firstly, a one-time examination of the product prior to export, and, secondly, the existence of key escrow or key recovery technology to circumvent the encryption. \(^{91}\)

It should be noted that the Administration is entitled to establish restrictions on export without the need for separate legislation, by virtue of emergency legislation. \(^{92}\) As will be seen below, today there is liberalization in the area of encryption exports from the United States. However, examination of the regulations shows that political, economic and security considerations influence the possibilities of export to various countries. The liberalization policy has continued, by means of a series of additional permits issued in 1998 and 2000.

The current legal situation

**Within the United States:** There is no restriction on production or commerce in the means of encryption of any strength within the United States. **Outside the United States:** Regulation by means of export regulations implemented by the Bureau of Export Administration (BXA). The BXA is responsible for the administration of the export of encryption items. \(^{93}\) The only blanket prohibition that remains in force is that relating to export of means of encryption to states that support terrorism, or their citizens. \(^{94}\)

---

\(^{89}\) 61 FR 68572 (1996), http://w3.access.gpo.gov/bxa/fedreg/ear_fedreg96.html#encryption

\(^{90}\) For a technical explanation of DES, see Section B in this chapter.

\(^{91}\) These terms mean that a third party, who is not the owner of the encrypted information, will have the possibility of deciphering the information. The regulations define who can be the third party, and the manner in which that party can be applied to in order to decipher information.


\(^{94}\) The states supporting terror, according to the American Government, are: Syria, Iran, Iraq, Libya, Sudan, North Korea, and Cuba. Additional information relating to the policy of defining states as terror-supporting can be found in a document by the Congressional Research Service from March 2001, which deals with Terrorism and United States Foreign Policy: http://www.fas.org/irp/crs/IB95112.pdf. An additional explanation can be found at the State Department website: http://www.state.gov/ww/global/terrorism/1999report/sponsor.html.
Permits in 1998.\textsuperscript{95} The most significant step in this year was the Administration’s waiver of the blanket requirement for the means to decipher encrypted messages (back door). A further step was the strengthening of the technological defenses of financial institutions. Following is a list of some of the changes implemented in that year:

- It is permitted to export, subject to license and after examination, technologies integrating means of encryption, to banks and financial institutions (including insurance companies), in 45 countries,\textsuperscript{96} without the means of decipherment,\textsuperscript{97} and without restriction on the strength of encryption. This permit is designed not for mass-marketing products, but for a limited market and for the purpose of carrying out secure transactions between financial institutions and their clients.

- An export permit for all encryption up to 56-bit strength after technical examination.

- It is permitted to export encryption to American subsidiaries or branches of American companies outside the United States.

- It is permitted to export encryption technologies for electronic commerce, under license, to 45 countries, on condition that the transactions are secured and that direct customer-to-customer communications are not carried out.

- A permit to export encryption commodities or software for health and medical uses, to 45 countries, without limitation on the strength of encryption, provided these are designated for end-users only.

- Anybody who received an exemption from export restrictions for 40-bit encryption may upgrade the product to a 56-bit product.

Permits in 2000.\textsuperscript{98} The most recent changes have led to a much more liberal situation in regard to the export of encryption items, in particular to the countries of the European Union and a number of other countries. Under the new restrictions, it is

\textsuperscript{95} See 63 FR 50516 (09.22.98), 63 FR 72156 (31.12.98), found at: http://w3.access.gpo.gov/bxa/fedreg/ear_fedreg98.html#encrpt.

\textsuperscript{96} See: Supplement No. 3 to (EAR), 15 C.F.R. Sections part 740. Today this Section no longer appears, since the restrictions are no longer unique to these countries.

\textsuperscript{97} Key escrow or key recovery.

\textsuperscript{98} See 65 FR 62600 (19.10.00), 65 FR 2492 (14.1.00), available at http://w3.access.gpo.gov/bxa/fedreg/ear_fedreg00.html#65fr2492. See also the statement by the White House regarding the change in policy relating to the export of encryption: http://www.cdt.org/crypto/CESA/whousepress091699.shtml.
permitted to export products and software that include encryption of any strength to companies, individuals and non-governmental organizations without license and after a technical examination only. The arrangement of examination prior to obtaining an export license, the requirement of integrating decryption means and licenses has been replaced with a mechanism for examination at an early stage, and post-export reporting requirements, in order to provide the Administration with information regarding where the encryption technology has been exported to, and of what strength. The regulations make it easier for communications companies and Internet service providers and allows them broader use of encryption. Producers of short wave radio technologies also benefit. Following are some of the key changes:

- The new regulations permit the export, after the Administration’s examination, of products or software with encryption of any strength, to individuals, companies other non-government end-users. Similarly, it is permitted to distribute encryption to all destinations, since uploading of an encryption item to the Internet does not constitute “knowledge” of transfer of encryption to a terror-supporting state. The amendments allow the exporter to simply notify the Administration that encryption means have been exported.\(^9\)
- The regulations simplify export to countries of the European Union and additional countries in Europe, as well as Japan, Australia and New Zealand.
- The regulations simplify the export of encryption items designed for short wave radio technologies.
- It is permitted to export encryption items to American companies outside the United States without prior technical examination. Encryption companies operating in the United States that employ foreign nationals no longer require an export license.
- It is permitted to export Open Source Code subject to license, and the Administration must be notified regarding the location of the code.\(^{10}\)

\(^9\) The Bureau of Export Administration (BXA) recently fined a software company, NeoPoint, for knowingly exporting, without a license, 128-bit encryption software to South Korea. See: http://www.bxa.doc.gov/press/2002/PenaltyImposedExpEncSoft.html.

\(^{10}\) Open Source Code is code in machine-readable language (See Computers Law, 5745-1995, Section 1, Definitions), which may be modified or from which encryption algorithms can be extracted. The term “open” means that the code is accessible to the public, and is not for commercial purposes, such as the Linux operating system.
• The regulations permit communications companies and Internet service providers to integrate encryption in the services they provide.
• In most cases, there is an obligation to allow the BXA a (one-time) examination of the product.

Criticism of the Administration
The Administration’s recent changes (in 2000) lessened the criticism of the system by human rights and privacy organizations. The Center for Democracy and Technology,\(^{101}\) published two criteria by which, in its opinion, the policy should be measured: Firstly, the extent to which the export regulations limit people around the world from using encryption technology in order to protect their privacy; and secondly, the freedom given to individuals to participate in the information economy without contravening U.S. law. On the basis of these criteria, the Center raises certain criticisms of the new regulations, in four areas: \(^{102}\)

• The export permit is only granted for products that are “sold” (for payment), which means that there is no express permit for free distribution of products containing encryption items, including products such as secure internet browsers, which are distributed online at no charge.
• The broad definition of “government,” which includes any state-owned or related organization or corporation, places too high a demand on small businesses and individuals who would like to export strong encryption products to those bodies that are, unjustifiably, defined as governmental.
• The reporting and screening obligations, to prevent strong encryption technologies from reaching terrorism-sponsoring states, handicaps medium and small organizations and individuals from distributing these technologies. The reporting obligations regarding the destination of these technologies have to take into account the fundamentally anonymous distribution of technologies through the Internet.
• The restrictions on export of encryption-related source code\(^{103}\) affect the distribution of non-commercial source code, designed for use and development by large numbers of users. Companies and organizations may be able to cope with the

\(^{101}\) http://www.cdt.org.
\(^{102}\) See details of the Center’s position in the letter to the BXA: http://www.cdt.org/crypto/admin/991206comments.shtml.
\(^{103}\) This refers mainly to encryption algorithms found in machine-readable source code.
restrictions. However, the distribution of source code that is “not subject to any proprietary commercial agreement or restriction” creates problems of enforcement, and the imposition of the restrictions on everyone involved in developing the code is not practical.

3. The International Scene

After examining the situation in Israel and the United States, we turn to review the legal framework on the international scene, where we note a clear trend toward limiting (or even abolishing) control over encryption products and services.\(^{104}\) This trend has found expression in certain countries, and in most countries of the Western world, it is now possible to freely create, use and sell encryption products and encryption services. This sub-chapter will briefly review the activities of policymaking bodies on the international scene and specific national provisions.

**Key Organizations Involved in the Formulation of International Policy**

In line with the international report on encryption,\(^{105}\) we can identify two bodies as the key players in rejecting limitations on encryption and developing a competitive, open market for encryption products: **the European Union (EU) and the Organization for Economic Cooperation and Development (OECD).**

**a. The European Union (EU)**

In 1992 the European Union Commission established a committee to study the issue of information security and encryption, as part of a program that included a strategic working framework for information security; analysis of data protection needs; provision of solutions for those needs; specification, standardization and verification of information security; integration of technological developments in the area of data protection; and integration of security functions in information systems.\(^{106}\) The Commission published a number of reports and position papers,\(^{107}\) which indicated an intention to develop a strategy to protect the internal market for encryption products and associated services, as well as creating a framework that will protect those who

---

\(^{105}\) Ibid.  
\(^{107}\) http://europa.eu.int/scadplus/leg/en/lvb/l24121.htm
choose to utilize encryption products in appropriate frameworks. These position papers were indeed translated into a number of directives, some of which will be reviewed below.

One expression of the trend toward a free market for encryption products and encryption services can be found in the Directive on Electronic Signatures (Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures).\textsuperscript{108} The issue of electronic signatures and the commercial bodies involved in the process toward gaining recognition for such signatures is closely connected with the area of encryption, since all certification processes are based on encryption keys. The definitions section of the directive gives explicit and formal expression to concepts related to the encryption process used in verifying electronic signatures: signature-verification data (including codes or public encryption keys used to verify an electronic signature); signature-verification devices (configured software or hardware used to implement signature-verification data); and digital certificates, which are electronic attestations which link signature-verification data to a person and confirm that person’s identity.

Sections 3-4 prescribes that the Member States may not introduce restrictions on the entry into the market of certification providers, nor establish any requirement for prior authorization before receiving the necessary governmental permits. At the same time, voluntary schemes may be introduced to enhance levels of certification service. All conditions related to such schemes must be objective, transparent, proportionate and non-discriminatory. Similarly, a supervisory system for service providers needs to be set up. Among other things, the Commission requires member states to report to the Commission on any national proposal to impose rules or restrictions on encryption products.

\textsuperscript{108} OJL 013 (19.01.2000) pp. 0012 – 0020
b. Organization for Economic Cooperation and Development (OECD)\(^\text{109}\)

In 1997 the OECD (Organization for Economic Cooperation and Development) published guidelines for encryption policy.\(^\text{110}\) The guidelines are directed mainly at governmental authorities, but are written with the expectation that they will stimulate interest from both the private and the public sector. These are the principles listed in the document:

1. Encryption methods should be trustworthy in order to generate confidence in the use of communications systems.
2. Users should have the right to choose any encryption method, subject to applicable law.
3. Encryption methods should be developed in response to the needs and demands of the target audience.
4. Technical standards for encryption should be developed at the national and international level.
5. The fundamental right to privacy, including secrecy of communications and protection of personal information, should be respected in national encryption policies and in the implementation and use of the various methods.
6. National encryption policy may permit legal access to the non-encrypted text (plaintext) and to encryption keys.
7. The responsibilities of bodies providing certification of encryption services or holding or accessing encryption keys need to be clearly stated.
8. Governments should cooperate to coordinate encryption policies. To this end, governments should remove, or avoid creating in the name of encryption policy, unjustifiable obstacles to trade.

Note particularly the third principle, which relates to the need for the development of encryption methods, based on the requirements of the free market (market driven development of cryptographic methods). This principle states that research and development in encryption need to be dictated by the needs, requirements and

\(^{109}\) Organization for Economic Cooperation and Development. This is a forum established in 1961, and based in Paris. The organization includes the 29 developed nations (Israel is not a member). This international forum publishes guidelines on various topics related to economics and trade, and these recommendations, although not officially binding, have a great deal of influence on the member states, as well as on states that are not members of this forum. See: http://www.oecd.org.

responsibilities of individuals, businesses and governments. This ensures that developments keep pace with changing technologies, the demands of users, and market developments in general.


Along with rejection of approaches based on local or national frameworks, most countries have rejected Key Escrow (Key Recovery) policies (the idea by which users may use encryption in their systems, but a third – governmental – party would receive the keys to the code from encryption services providers, and that government body would be responsible for providing the keys to the appropriate authorities when asked to do so). This policy was adopted under French law in 1996, but the law was repealed in 1999. This policy was also promoted for a few years by the British government (we will return to this point later). The United States tried to promote this policy, but met with rejection on the part of the OECD, as well as criticism from security experts who emphasized the problematic nature of a situation in which a central body held the encryption key, with the main points being the issues of voluntary compliance, privacy, cost and effectiveness. The final rejection of this policy came in the Wassenaar agreements of December 1998 (see below). Today, only a few countries apply this approach, and in the United States – as discussed above – the export restrictions that encouraged such an approach were repealed in January 2000.

As a result of the rejection of Key Escrow policies, a new approach was adopted by many countries: the demand for “lawful access” to encryption keys or message plaintext. Under this approach, individuals may be asked to reveal encryption keys to law enforcement authorities, and, if they refuse, they may be liable to criminal prosecution. Up to the year 2000, only a few countries had enacted laws of this type, but now the situation is likely to change. The OECD guidelines described above noted the principle of “access”, but did not necessarily support it. The guidelines noted that national policy may permit legal access to the plaintext or encryption keys, but this policy had to respect the other principles appearing in the organization’s guidelines.
This issue provoked sharp debate within the framework of the OECD, until the organization finally decided not to support a global approach to “legal access.”

In the context of the “lawful access” approach, consideration should be given to the privilege against self-incrimination, which is well founded and binding in many countries in the world. Underlying this privilege is the prohibition on governmental bodies to coerce an individual into giving testimony that may incriminate him. In this context, there exists the argument that, in light of this privilege, it is not possible to coerce individuals to reveal encryption keys or passwords not recorded elsewhere. In the United States this argument has been raised in connection with the Fifth Amendment to the Constitution, while in Europe the argument is based on the European Convention on Human Rights, which permits an individual to retain his right to remain silent.

d. The Wassenaar Arrangement

The Wassenaar Arrangement is a series of agreements between 33 states to control the export of conventional arms and “dual use” (usable for both commercial and military purposes) goods and technologies. Under the heading of technologies is included a number of encryption products which are considered “dual use.” It should be emphasized that this is not a convention or type of legislation, but the exchange of opinions at the international level. Thus, compliance of the participating states is a matter for each state’s consideration, and is carried out by means of legislation at the national level. The main provisions of the Arrangement relate to the free export of encryption products based on key length, the easing of restrictions on the export of products encrypted in order to protect intellectual property rights, and provisions under which the export of encryption products not mentioned in the agreements requires a license. This is important in light of the fact that today there exists a

\[111\] See, for example: Doe v United States, 487 US 201, 219 (1988) (Stevens J, dissenting) (“[a defendant] may in some cases be forced to surrender a key to a strongbox containing incriminating documents, but I do not believe he can be compelled to reveal the combination to his wall safe – by word or deed.”).


\[113\] www.wassenaar.org.
significant loophole that allows free trade and distribution of non-tangible encryption assets, including by means of downloading from the Internet.\textsuperscript{114}

e. International Categorization

In the framework of the international report mentioned above, countries are categorized in respect of the means of control applicable to trade in encryption products and services.\textsuperscript{115} The report divides the countries that were investigated into three categories, on the basis of how they control encryption. This categorization is designed to allow a world map of encryption policies to be drawn up for purposes of comparison. There are no accompanying sanctions to this categorization.

The “green” category includes those countries that promote a policy that allows trade in encryption products without legal impediments, such as where the country has adopted the OECD guidelines. The “yellow” category applies to countries that have proposed state controls over encryption, including limitations on use or import, or where the country operates strictly within the provisions of the Wassenaar Arrangement. The last category – the one considered least desirable – is the “red” category, and this includes countries that impose sweeping restrictions on encryption. Many countries don’t fit exactly into one or other of the categories, and so the report, where appropriate, lists certain countries between the different categories.

In line with this categorization, Israel was classed in 1998 under the “red” category, that is, the category with the most restrictions on encryption. In 1999 there was an improvement, and the category level was changed to red-yellow; in 2000 Israel was ranked as “yellow,” that is, in the intermediate group.

f. The Legal Position in Britain

The United Kingdom adopted in May 2000, a law implementing the European Directive on Electronic Signatures (99/93/EC) came into effect. This is the

Cryptography Service Provider and the Electronic Communication Act 2000. The British law establishes a series of actions that need to be carried out toward the registration of encryption service providers, and also establishes legal recognition of electronic signatures. In line with the provisions of the law, the Secretary of State is required to establish and operate a **Register of Encryption Service Providers**.\(^{116}\) Companies that will be entitled to registration are those that provide services such as public key verification for individuals, administration of encryption keys, timestamping services for electronic signatures, storage of encryption keys, and so on. Although the law does not provide specific criteria for registration approval, it does list the necessary details to be submitted upon application, among them the proposed technology, the identity of the applicant for registration, and the means by which the applicant will offer the technology to the public. This law, in fact, explicitly rejects the key escrow approach. Rather, it adopts the approach of keeping a register of service providers that is open to the public, as opposed to a secret government register that would collect the keys themselves.

A key aspect of the law is the fact that the register is voluntary. As a result, any provider of encryption services could trade in the open market without reference to the fact that its name is absent from the public register, or even if its application for registration has been rejected. At the same time, it should be remembered that the significance of the register being public is the fact that it is open to public scrutiny and examination, and thus serves as a tool to assist in selection and review in this area.\(^{117}\)

4. The International Scene – Decryption

Now that we have looked at direct systems of regulation as they relates to encryption, we can turn to the other side of the coin: the questions that arise when encrypted material is deciphered by a third party. Where a person wants to protect certain information, she may chose to do so in a number of ways. Thus, digital protection mechanisms may be found when one enters an e-commerce site or server – in the form of a password. Or, in the home, such mechanisms may be found in the form of a password.

\(^{116}\) Encryption service providers are defined in Section 6 of the law thus: “Any service which is provided to the senders or recipients of electronic communication, or to those storing electronic data, and is designed to facilitate the use of cryptographic techniques.”

Pay TV decoder, or built into the products themselves, in order to limit their functionality. Each of these systems requires decryption in order to access and use the information.

International law regarding decryption has been enacted in three main frameworks: protection by means of legal frameworks that complement intellectual property rights (copyright), legislation related to conditional access to encrypted services, and legislation dealing with databases.

**a. Para Copyright**

Copyright, in essence, provides its owner or holder with the right to control certain specified uses of his work. In recent years, various devices have been developed to offer technological protection of works, and the law now recognizes the right of the copyright holder to use such devices to protect her work in situations where others would like to circumvent those devices. We will now present the main legal arrangements that provide a preferential status for technological means used for protecting copyright. We will look at how copyright law protects encrypted material from decipherment, in light of various pieces of legislation: the WIPO treaty, the American DCMA law, the activities of the European Union in respect of ratifying international treaties, the new European Directive on Copyright, and, finally, the position of British law on this issue.

**WIPO Copyright Treaty, WIPO Performances and Phonograms Treaty**  
These treaties are the work of the World Intellectual Property Organization. Underlying the organization’s treaties are the Paris and Berne Conventions, and subsequent treaties, including these (signed in 1996) expanded the protection offered, taking into account developments in digital technology. The WIPO Copyright Treaty (WCT) and WIPO Performances and Phonograms Treaty (WPPT) are aimed at updating the international protection given to copyright and related rights in the

---

118 See: http://www.wipo.int/treaties/ip/copyright/copyright.html.
Internet age. The first is already in effect, while the second is expected to come into effect in the near future.

In accordance with the WCT, the author of a work is entitled to legal protection in respect of distribution, commercial rent and public broadcast of her work over a network. Specific protection is given to systems for identifying and managing works. Section 11 of the treaty requires signatories to provide protection against the circumvention of effective technological measures that protect the author’s rights or which prevent acts that are not authorized by the author or which are not permitted by law.

**The Digital Millennium Copyright Act (DMCA)** ¹¹⁹

As part of bringing American law into line with the 1996 WIPO Copyright Treaty,¹²⁰ Congress passed the DCMA in 1998. This law is designed to prevent the circumvention of technological measures that protect copyright works. The heart of the prohibition is in Section 1201, which prohibits the circumvention of technological access measures:¹²¹

“No person shall circumvent a technological measure that effectively controls access to a work protected under this title.”

In addition, the law prohibits the production, sale, provision or distribution of any measure that, wholly or in part, is designed to circumvent technological measures that protect copyrighted materials:¹²²

“No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that – (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;”

---

A question of interpretation that has not yet been tested in the courts is that of the scope of the prohibition: does the law apply to the decryption of technological protections in general, or only those technological measures that protect works which are themselves protected by copyright law. The prohibition against deciphering technological protections is not limited to local (American) technologies, and therefore the deciphering of a protective technology that originates outside the United States is also an infringement of the law. The law establishes a civil offense, but where the infringement has been carried out for commercial advantage or private financial gain, then the infringement is also a criminal offense. The law establishes a number of general protections or defenses, notable among them being the protection given to certain research, examination and evaluation of protection mechanisms:

- The law does not override the authority of the Administration, intelligence services or law enforcement agencies to carry out activities for the purpose of investigation, protection, data protection and intelligence gathering.
- There is an exception that permits the circumvention of technological access protections, for the purposes of research aimed at finding flaws and vulnerabilities in encryption technologies. This exemption was inserted because of the concern of lawmakers that the prohibition of decryption of access protections would hamper the development of research into the flaws in existing technologies.
- The “fair use” defense does not justify decryption in contravention of the provisions of the section.

The first criminal prosecution under this law was against a Russian citizen, Dmitri Sklyarov, who developed a program that bypasses the technological defenses of eBook, a technology that belongs to Adobe. The program was developed for a Russian company named ElcomSoft, which was also named as a defendant. In

---

125 17 U.S.C. §1201(g).
126 See the reports of the various Congressional committees: H.R. Rep. No. 105-551, pt. 2, at 27 (1998); S. Rep. No. 105-190, at 15 (1998). The legislature demanded a report, one year after the law took effect, on whether the law indeed had a negative effect on encryption research. According to the report, it is still to early to draw conclusions. See: http://www.loc.gov/copyright/reports/studies/dmca_report.html#N_12_.
128 For details of this case, see: http://www.eff.org/IP/DMCA/US_v_Elcomsoft/.
130 See the company’s website:http://www.elcomsoft.com.
December 2001 a plea bargain agreement was signed, and the prosecution agreed in effect to waive Sklyarov’s prosecution without a conviction being recorded.\footnote{Sklyarov undertook to testify against ElcomSoft. The court papers related to the plea bargain can be found on the Justice Department’s website: http://www.usdoj.gov/usao/can/press/assets/applets/2001_12_13_sklyarov.pdf}

The law has so far been interpreted in the framework of a number of civil actions:

- Film companies sued to prevent websites distributing the code that breaks the technological protections of DVD movies. Arguments regarding fair use and the unconstitutionality of the DMCA — in that it is restrictive, to a large extent, of freedom of speech — were rejected by the court of first instance and the court of appeals.\footnote{See: \textit{Universal City Studios, Inc. v. Reimerdes}, 111 F. Supp. 2d 346 (S.D.N.Y. 2000), aff’d \textit{Universal City Studios, Inc. v. Corley} 2001 WL 1505495 (2nd Cir. 2001). For more on freedom of speech, see section E.4 in this chapter.}

- In another case, also related to the question of DVD encryption, the Californian state courts dealt with the question of decryption in light of laws protecting trade secrets.\footnote{Trade Secret Act, Cal. Civ. Code, § 3426.1 et. seq.} An interim decision removed the restraining order that prohibited distribution of the decryption code through websites. In this case the court stated:

  “DVDCCA’s [The Plaintiff] statutory right to protect its economically valuable trade secret is not an interest that is “more fundamental” than the First Amendment right to freedom of speech or even on equal footing with the national security interests and other vital governmental interests that have previously been found insufficient to justify a prior restraint.”\footnote{\textit{DVD CCA v. Bunner} 93 Cal. App. 4th 648 (2001).}

- Another case related to a researcher who wanted to publish his research, and was threatened with action under the DMCA. Professor Edward Felten cracked the protection technology of digital watermarks, in the framework of a public competition sponsored by the developers of the protection scheme. Felten waived the prize, and wanted to publish the results of his research. However, he claimed, the music industry (the RIAA) threatened to sue him under the DMCA. Felten applied to the courts for a declarative judgment that would recognize his right to publish his research as a part of his right to freedom of speech. Although the
District Court of New Jersey rejected his claim, the music industry declared that it did not object to the publication.

The trend that appears to be developing in American law is to prohibit the decryption of codes that protect works subject to copyright protection. It is not yet possible to draw any conclusions regarding the prohibition of decryption in the framework of trade secret protection. Given the statements of the court, quoted above, according to which the right to protection of an economically valuable trade secret is not more fundamental than the protection of free expression, one might wonder whether the protection of copyright is more fundamental than freedom of speech, and whether it is reasonable that the balance between freedom of speech and copyright is covered by arrangements in the copyright law.

The European Union

In a decision of the European Union – Council Decision of 16 March 2000, on the approval on behalf of the European Community of the WIPO Copyright Treaty and the WIPO Performances and Phonograms Treaty – the Council of Ministers ratified on behalf of the European Union the two WIPO treaties (WCT and WPPT, see above). It also empowered the Commission to act on this issue at various levels as representative of the European Union. In line with this decision, the European Union as such can now become a party to the WIPO treaties relating to copyright and related rights.


The aim of this directive is to adopt legislation in respect of copyright and related rights in a manner that reflects technological developments, and, in particular, the Information Age. It also introduces the WIPO treaties (discussed above) into EU law.

135 Felten v. RIAA (D.N.J.)
136 http://www.wired.com/news/politics/0,1283,48726,00.html
137 OJL 167 (22.06.2001).
The Directive deals with three main areas: copyright, public broadcast and transmission rights, and distribution rights.

For our purposes, what is important is the legal protection that the member states are required to provide against the circumvention of effective technological means that protect copyrighted works. Additionally, the legal protection relates to preparatory acts, such as production, import, distribution, sale or provision of services, that circumvent technological protections. Another provision relates to rights-management information included in the copyrighted work, that is, information about the copyright owner, or the terms and conditions for use of the work. The Directive provides legal protection for such technological measures as are taken by copyright holders to prevent illegal modification or circumvention.138

Britain

The British Copyright, Designs and Patents Act 1988 establishes, in sections 296-297, a prohibition against development, import, sale, rental or advertisement of any device or measure aimed at circumventing the protection against copying a protected work. The broad terms of the prohibition include the publication of information that assists in carrying out acts designed to circumvent such protections. In addition, the law also prohibits unlicensed decryption.139

A recent British judgment is also interesting. The case of Mars UK v Teknowledge Ltd140 dealt with a claim for breach of confidentiality by means of reverse engineering of a device that held encrypted data. In line with the requirements developed in a previous judgment,141 the court found that the encrypted information itself was not confidential, seeing that the device (Cashflow) was available to the public, and that there were no special circumstances that suggested an obligation to maintain confidentiality on the part of the respondent. Of importance here was the fact that the machine was commonly available, and thus one might say that, when considering the transmission of encrypted data, which is not commonly available,

141 Coco v. AN Clark [1969] RPC 41.
there might exist the possibility of ruling that the information is confidential. What the judgment makes clear is that encryption itself does not make encrypted material confidential, in the absence of any other relationship between the source and the decoder.\textsuperscript{142}

b. Conditional Access
A second means of protecting copyrighted material, and, consequently, protecting encryption methods and restricting decryption, is the legal protection given to technological services that operate on the basis of restricting access to content. A 1998 European Directive establishes a uniform legal framework for proceeding against devices or services that provide unlicensed access to copyright protected services such as television, radio, cable transmissions, satellite transmissions, electronic publication and so on, where such services are provided to the public on the basis of subscription or payment for viewing.\textsuperscript{143}

“Illicit device” is defined as any equipment or software designed to give access to a protected service (Article 2(e)) in an intelligible form without the authorization of the service provider. “Infringing activities” include the manufacture, import, distribution, sale, rental or possession for commercial purposes of illicit devices. The installation, maintenance or replacement for commercial purposes of illicit devices is also prohibited. The member countries of the European Union are also prohibited from restricting the protections afforded to protected services that originate in another member country, and from restricting the free movement of conditional access devices, except those defined as illicit. The member countries are required to enact internal legislation, in line with the provisions of the Directive, by 28.05.00.\textsuperscript{144} England, for example, implemented the Directive in the framework of its Copyright, Designs and Patents Act 1988 (CDPA).\textsuperscript{145}

\textsuperscript{142} \textit{E-commerce: A Guide to the Law of Electronic Business}, supra note 114, at pp. 63-64
\textsuperscript{144} http://europa.eu.int/scadplus/leg/en/lvb/l26050.htm
Note that, in spite of the broad definitions found in the Directive, it is not clear whether passwords obtained illicitly fall into the category of “illicit devices,” since a password is not necessarily a device, nor is it software designed to provide access to the protected service.\footnote{146}{E-commerce: A Guide to the Law of Electronic Business, supra note 114, at 71.}

c. Databases

A third means by which encryption is protected – such that there exists a legal restraint on decryption – is by means of the protection given to databases. The European Union has a Directive for the legal protection of databases that provides such protection – \textit{Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases}.\footnote{147}{See: OJL 77 (27.03.96).}

The Directive creates, in a framework separate from traditional copyright laws, a new intellectual property right in respect of databases. This new right is based on the substantial investment (measured qualitatively or quantitatively) in obtaining or verifying the material in the databases, as opposed to the criteria of creativity and originality required for protection under copyright law. The Directive prohibits the extraction or other use of information in such amounts as would be deemed qualitatively or quantitatively significant (Article 7(1)). It also establishes a prohibition of extracting data from a database and of reusing such data in any manner or in any forum, thus creating an effective prohibition against breaking the encryption of such material. The fair use protections in respect of this right have been narrowed. Permitted uses include the extraction for private use of data from a non-electronic database, for purposes of teaching or scientific research, and for purposes connected with public security and/or judicial procedure (Article 9). This last protection – a specific exception aimed at public security needs – permits the extraction of data from a database for security purposes, and such an act will not be deemed an infringement of the intellectual property rights that exist in respect of that database (these rights are
in addition to the copyright protections applicable to the database as a result of originality of design or arrangement of the data).  

E. Implications and Policy Considerations

We are now familiar with the technical nature of encryption, and its capabilities and limitations. We have looked at the security needs that underlie both the motivation to encrypt and the motivation to prevent others from using encryption. We have also reviewed the legal arrangements, in Israel and overseas, in respect of encryption and decryption, and mentioned their scope and the developing trends in those legal frameworks. What remains is to reflect on those considerations that should serve as guidelines for formulating an appropriate policy in this area. These considerations include, apart from the security considerations that underlie the whole arrangement, economic considerations – both in the narrow sense (the market for encryption products or electronic commerce) and in the broader sense (intervention in the free market) – and human rights considerations, ranging from the right to privacy and freedom of speech to property rights and freedom of occupation. An in-depth, focused examination of the range of considerations will actually afford, in the end, a broader viewpoint, and will assist in formulating policy guidelines for the most desirable legal arrangement.

1. Market Intervention and Research and Development Considerations

a. The influence of governmental intervention on research and development

In the area of encryption (and computers in general), constant development has far-reaching economic significance. Hi-tech companies have to constantly innovate and update their products in order to remain competitive (the average time between the release of one product and the next is 18 months). This is true particularly when we consider methods of encryption and protection for systems, since there is a constant, parallel, effort to develop the means to break through them.
Those involved in this area in the private sector have a clear interest in developing their products without any restrictions and in line with the demands of the market. At the same time, because of other interests (some of which we have discussed previously, such as defense, and others which will be examined below, such as privacy and freedom of information), there arises a dilemma as to the appropriate level of regulation for this area. The question that needs to be examined in regard to research and development is: what economic influence would regulation have on incentives for private companies, and is this a desirable situation for them and for the market as a whole?

b. Restrictions on export of the means of encryption and the use thereof

This approach, of governmental non-intervention, is the desired approach from the point of view of industry, and not only in the area of research and development. Consideration of this issue can be found in connection with regulation schemes affecting encryption in general, and those that restrict export of the means of encryption in particular. During that period when the restrictions were more stringent, computer companies came out against them and called for reform. Their call was supported by the argument that these restrictions had a serious economic effect on American companies. For example, the CSPP (Computer Systems Policy Project)\(^{149}\) called for a change in policy and an opening of borders, since export restrictions affected the ability of American companies to compete effectively in world markets.

In addition to export restrictions, regulation of encryption may take the form of various prohibitions regarding its use by anyone other than the authorities, or of restrictions on the level of development permitted in the field. Since the area of decryption is constantly development (and will continue to develop, even in the event that it is prohibited, by elements that are not law-abiding), the implications of these two situations are similar: private bodies and individuals will no longer enjoy the protection of their data.

\(^{149}\) [http://www.cspp.org/Reports.asp?FormMode=Call&LinkType=Text&ID=9565291994](http://www.cspp.org/Reports.asp?FormMode=Call&LinkType=Text&ID=9565291994)
Koops\textsuperscript{150} considered the possibility of a prohibition being imposed on encryption. In his view, when a problem arises in society as a result of a particular element, the natural tendency of the state is to make that element illegal. This is logical when dealing with an element or activity, all of whose results or influences are negative (such as murder). However, encryption also has many positive aspects. Thus, Koops holds that making encryption illegal is not a realistic option. Nonetheless, the suggestion to prohibit encryption has been raised by a number of governments around the world, and this is why Koops dealt with it.

Prohibition may be absolute or partial (licensing of weaker encryption, or only to certain bodies). However, whatever the case, such prohibition is not enforceable, and would create a situation in which it would be criminal and terrorist elements who would continue to make use of encryption. Those who would be most affected by the prohibition would be law-abiding citizens. Apart from the harm done to individuals (privacy issues, and the balance of power between the citizen and the government), there would also be harm on the collective level, and this would be reflected in economic damage: international trade would be affected, since companies would not be able to communicate securely with each other. In addition, if the prohibition were only on a national level, and not enforced globally, companies in countries that impose such a prohibition would not be able to compete with their counterparts from other countries – thus damaging the economies of those countries restricting encryption.

This examination of the various implications suggests that regulation of encryption, in whatever form, is not economically effective. Economic theory makes it clear that the market operates best when it is free, without any intervention. The picture changes, of course, when there are market failures. Then there is a need for governmental intervention. The question is, whether terrorist activities concealed by encryption, and the breaking of encryption by hostile elements, constitute market failures that would require (from a purely economic point of view) intervention. It appears that, in the view of the computer industry – and even certain international bodies – the best way

of dealing with the problem is to allow industry to continue developing protections against such threats under competitive market conditions.

2. The Influence of Encryption Regulation on Electronic Commerce

An additional economic effect that may occur as a result of restrictions on encryption, is in the area of electronic commerce or trade. According to a theory proposed by Schilling, and based on game theory, where regulation is increased, the level of use of the Internet by private users will decrease. This would occur in spite of the public’s interest in preventing crime and fighting terrorism. A high level of regulation would limit the options for encryption that exist in the market, and without strong encryption protecting their privacy, users would not feel sufficiently secure in using the internet for commerce. A similar argument was raised in a document submitted to the American government by EPIC (Electronic Privacy Information Council), in the framework of public comment regarding the desired policy regarding electronic trade. According to the recommendations presented in this document, the Administration should avoid regulatory intervention in the area of encryption, and let the market develop strong encryption tools. It is only this approach that will encourage use of the internet in general, and participation in e-commerce in particular. The significance of this statement is that the developing area of e-commerce, which is an effective and desirable economic tool, will be directly harmed and will lose its effectiveness, if the state were to impose broad restrictions on encryption.

3. The Right to Privacy

Encryption is a mechanism which, on a conceptual level, protects the user’s privacy. Encryption and encryption systems constitute a system of “doors and locks” in the digital environment, that protect increasing amounts of personal information,

---

151 Thorsten Schilling, “Raiding the Net: Is There a Need for an Information Highway Patrol?” 1 Netnomics 37, 51 (1999).
152 See: Public Comment on Barriers to Electronic Commerce- Comment on Behalf of Electronic Privacy Information Center (EPIC) by Sarah Andrews, and Andrew Shen (17.3.00), available at http://osecnt13.ossec.doc.gov/ecommerce/barriers.nsf/review/46112999BDD282C9852568A6000093AF
electronic mail communications, electronic commerce and other data that could be used to infer information that is considered private.\textsuperscript{153}

Encryption does not differentiate between classes of users or methods of use, and the same level or strength of encryption applies, for good or bad, both for the innocent user and the criminal or terrorist. If we stretch the doors/locks metaphor a little, then in spite of the fact that privacy principles (and property rights, which we will discuss later) would certainly support the right of each individual to protect his own personal information as much as possible, not everyone can build whatever fence, or install whatever lock or telephone line, he wants. There are always controls that restrict him – starting with the production of protective devices, their installation, and quality control – all the way to marketing. The reasons for this are many, and vary from one field to another. In abstract terms, regulation needs to take into account the extreme cases in society, and not the innocent citizen. For our discussion, this means the terrorist who, in the technological age, uses electronic communications and other methods protected by encryption, in exactly the same way as “old style” terrorists used physical items, protected or concealed by physical means of one kind or another. For both old-time devices (if one may use the term) and modern means, there have to be (and there are) ways of breaking into them, a kind of “back door,” held by governmental authorities – the state.

In spite of this parallelism, what makes encryption methods unique, is that they are designed \textit{ab initio} to conceal, and so it is not sufficient to grant specific authorization to break a certain encryption (as is done in the case of wiretapping, for example). It has to be ensured ahead of time that the technological possibility of breaking the encryption exists. Thus, regulation affects not only the user or the potential user (chilling effect), but also touches directly on the population as a whole. Regulation of the means of encryption well before the stage at which it is used – at the stage of production, import or sale of these means, for example – has an influence on all citizens as individuals, and on whole segments in the economy who are involved in

\textsuperscript{153} Section 2 of the Israeli Privacy Protection Law, 5741-1981, defines what constitutes a violation of privacy, and its provisions may also be applied to the digital environment. For example, Section 2(5) defines the copying or use of the contents of a letter or other document which is not meant for publication as a violation of privacy. Electronic mail could be included in this definition. In addition, there is the prohibition against illegal penetration of computer materials, under Section 4 of the Computers Law, 5745-1995.
the production and marketing of those means of encryption.\textsuperscript{154} A long-running debate on this issue took place in the United States. The key question was this: to what extent, if any, should the Administration be permitted, subject to various limitations (court approval, division of the implementing body into two, which would then hold the key jointly, etc.), to maintain the option of using “back door” access, that is, a kind of “master key” or algorithm that would allow the recreation of private keys. What is clear is that, as the level of supervision and control over local production and importation of encryption products grows, the more possibility there will be for the State to access encrypted material via these “back doors,” and thus the risk of violating citizens’ privacy will also grow.

The effect on the individual’s privacy as a result of giving the state (“back door”) control over encryption mechanisms can be shown on two levels: direct harm, and indirect damage.

\textbf{Direct harm} – Providing the technical and legal possibility of intercepting and deciphering encrypted materials (even if only in exceptional cases), and thus penetrating those “doors and locks,” may, in certain circumstances, harm even law-abiding citizens who are not even under suspicion. This could occur, for example, when the circumstances require examination of material or correspondence passing through an internet server (for example, through a server that serves thousands of innocent civilians, but also a suspected terrorist). This is in addition to the inherent violation of rights involved in police investigations directed at those who are still innocent, since they have not yet been proven guilty, and the harm done in cases of error.

\textbf{Indirect harm – the fact that the Government has control} over the means of encryption or the possibility of decryption, and the existence of back door access, even if never used, creates a certain hesitancy among the public: it may serve as a chilling factor that deters people from using digital databases, online services, electronic commerce, and so on, and this is something that will have influence on individuals, society and the economy.

\textsuperscript{154} As regulated, for example, by the Control of Commodities and Services (Engagement in Means of Encryption) (Amendment) Order, 5748-1998.
Therefore, the right to privacy granted to each individual and the public interest need to be balanced, and action needs to be taken in two areas, parallel to the two threats faced by privacy:

We conclude that the following approach should be adopted:

Regarding direct harm, measures should be taken that will permit the security authorities to respond to security needs, where this does not exceed the extent necessary.

- The purpose for which the violation of privacy is permitted needs to be clearly and explicitly defined, and limited solely to the needs of thwarting terrorism. It should not be permitted for the purpose of obtaining evidence after an incident takes place (unless there is the possibility of repetition of the terrorist act, in which case the issue again becomes one of prevention).

- An independent, external, review mechanism needs to be established. It would be appropriate for this to be prior judicial review, similar to the position regarding wiretapping. We propose that any authority that requests to use a “back door” penetration or other means of breaking encryption should apply to a court prior to doing so, and the court should weigh the extent of the need for such penetration or decryption against the direct harm expected as a result.

Regarding indirect damage, the extent of State intervention in the production and importation of technological measures needs to be defined, as well as the extent to which the State is entitled to obtain access to “back doors.” The narrower and more explicit the general arrangement regarding encryption is, the less the indirect impact on privacy.

It should also be noted that the non-provision of sufficient means of decryption (“back door”) or the establishment of too-rigid criteria and procedures for obtaining permission for specific decryption operation, could bring about an opposite result, and cause more harm to the privacy rights enjoyed by suspects and others. For example,
instead of deciphering e-mail correspondence, law enforcement authorities might use cameras or personal surveillance, whose impact on a suspect’s privacy is more extensive and less focused.\textsuperscript{155}

### 4. Freedom of Speech

The connection between encryption and freedom of speech can be understood in two ways. The first is direct, that is, that encryption itself is a form of expression, and is thus entitled to protection in the framework of freedom of speech laws.\textsuperscript{156} According to this approach, any restriction on encryption necessarily limits freedom of speech. The second way of understanding the connection is more indirect: in the absence of strong encryption, web surfers (and this includes companies and governmental bodies) may avoid expressing certain views, out of fear that their privacy may be compromised. Therefore, the absence of strong encryption and the regulation of encryption, which raise the fear that the State has access to encrypted information, have a chilling effect on free speech. The indirect effect has been discussed in the subsection dealing with privacy. Here we will focus on the issue of applying freedom of speech principles to encryption.

The first question that arises is whether software can be viewed as speech. If so, what is the scope of the protection to which software is entitled in the framework of the protections afforded freedom of speech? The fundamental difficulty is that software has two components: the first is an expressive component, and the second is a functional one. When a person creates a program, by means of which he attempts to break into a government computer, for example, or cause the collapse of a government computer system, and by his actions this person wishes to express some

\textsuperscript{155} Professor Michael Froomkin raises an alternative viewpoint, that relates to encryption itself, even before any governmental intervention. Froomkin claims that the very use of key escrow violates privacy in two ways: 1. There is now a third party involved in any communication, the party that issues private and public keys. 2. When a public key needs to be recreated, certain personal information has to be provided (here the reference is to governmental agencies wanting to recreate a public key, and not the owner of the key). This viewpoint is not related to the two threats to privacy which we have discusses (which are more closely related to governmental activities), but rather to the possible violation of privacy rights by encryption mechanism or by the producers of encryption products. See: Michael Froomkin, "It Came form Planet Clipper : The Battle Over Cryptographic Key 'Escrow'” 1996 U. Chi. L. Forum 15, available at http://www.law.miami.edu/~froomkin/articles/planet_clipper.htm.

\textsuperscript{156} Amitai Etzioni, The Limits of Privacy 80, 90 (New York, 1999).
sort of protest, it is not easy to determine whether this behavior is covered by the principle of freedom of speech.

These questions arose in the United States in two contexts that touch on the regulation of encryption: in regard to encryption software itself, and in regard to software that breaks encryption. American law has applied to this issue the doctrine developed in regard to “symbolic behavior.” This doctrine was developed at a time when such situations were a lot less “technological.” Nonetheless, they shared a common basis, such as the case where a person publicly burned his country’s flag, in order to protest some government policy, or as in a case that came before the United States Supreme Court in the 1960, the O’Brien case. \(^{157}\) Paul David O’Brien and others publicly burned their draft cards. They claimed that they did so in protest against the Vietnam War. O’Brien was arrested and a charger of burning his draft card, in contravention of a 1965 law. The Supreme Court rejected the argument that all behavior or actions can be considered as “speech,” when done in order to express some idea of position. Moreover, the Court analyzed the situation in which action (behavior) and “speech” (in its First Amendment sense) are intertwined, and came to the conclusion “that when ‘speech’ and ‘non-speech’ elements are combined in the same course of conduct, a sufficiently important governmental interest in regulating the non-speech element can justify incidental limitations on First Amendment freedoms.” This means that in this type of case we do not need to apply an absolute standard of protection for freedom of speech, as would be applied in a case of regulation of pure speech on the basis of its content. Rather, a somewhat lower standard, known as “intermediate scrutiny,” may be applied. \(^{158}\) Chief Justice Warren established a number of conditions for public regulation, which, if they exist, justify the limitation of First Amendment rights:

1. The regulation is within the constitutional power of the government;
2. The regulation furthers some important governmental interest;
3. The regulation is not designed to restrict freedom of speech;


\(^{158}\) American legal decisions accept three standards of evaluating the extent of protection for freedom of speech. The highest standard, “strict scrutiny,” is applied when the State prevents certain speech, or the discriminates between different types of speech based on their content. A lower standard, “intermediate scrutiny,” is used by the courts when the limitation on speech is not on the basis of its content; according to this standard, the court weighs the free speech rights of the speaker against the national interest in limiting that speech, with the weightier interest winning. The third, and lowest, standard is called “rational basis;” here the speaker has to show that State regulation does not have any logical basis.
4. The incidental limitation on freedom of speech is not greater than necessary to promote the governmental interest.
In that case, it was ruled that the law under discussion was not aimed at restricting freedom of speech, but rather at ensuring the effectiveness of the draft procedure (this is the governmental interest). Thus, O’Brien was not placed on trial for his opinions, but because of his behavior, which damaged the national interest.

The question arises whether it is possible to adopt the O’Brien ruling in the context of encryption software. American courts have not been consistent on this issue.

The first instance is known as the Karn case: Philip Karn, a programmer working on cellular technology, requested a permit to export source code for encryption algorithms on diskette. The same algorithms had not long before been published in book form. While the book had been declared by the Department of State and the Department of Commerce to be a freely exportable commodity, these same bodies ruled that the export of the code in digital form was prohibited, under the regulations controlling the export of encryption software. Karn appealed the Administration’s decision to the District Court in the District of Columbia.

His argument was that the diskette constituted “speech,” particularly since the program code included programmer comments, which were not aimed at the computer running the program, but to a human reader looking at the source code and trying to understand it. Since the issue is one of expression, the diskette is protected by the freedom of speech protections under the First Amendment. On this basis he argued that the prohibition against exporting the diskette is unconstitutional, and thus void. The court rejected his case. Although the court agreed that the protections offered by the First Amendment also apply to program code, it ruled that, when the restriction on speech is not content-based, but rather content-neutral, this implies that it is designed to restrict some other function that the speech serves, and is thus justified if meets the conditions established in the O’Brien case.

In this case, the court ruled that the O’Brien test was met: the regulation of software exports is within the government’s powers; it is not aimed at restricting freedom of speech, but at promoting an important governmental interest.

---

159 See: Schneier, supra Note 25.
161 Karn, ibid. at 10.
(here, to make it difficult for hostile states to interfere with the access of the United States government to information essential for national security); and the incidental limitation on freedom of speech is in appropriate measure.\textsuperscript{162} It is important to note that Karn attempted to argue that the O’Brien test applied only to behavior that included in it speech. However, the court rejected that argument, and ruled that the test applied to any form of expression.\textsuperscript{163}

The Bernstein case led to a contrary decision, in which freedom of speech had the upper hand. Daniel Bernstein is a mathematician researching cryptography at the University of Illinois in Chicago, and at Berkeley in California. As part of his academic work, he developed a novel encryption algorithm, which he called “Snuffle.” Bernstein wanted to distribute and export the program he developed, accompanied by an article in which he analyzes and explains the program code. He also wanted to raise his findings at academic conferences, including some outside the United States. His intention was to disseminate his ideas within the scientific community throughout the world, as part of the normal academic exchange of ideas and information. The Export Regulations prevented Bernstein from publishing or discussing his work, and, in his opinion, harmed his career and reputation. In particular, his freedom of speech rights were violated. In 1996, Bernstein appealed to the United States District Court in California. Judge Marilyn Hall Patel ruled, firstly, that the encryption program was speech protected by the First Amendment, since anything written in any language is, by definition, an expression entitled to constitutional protection.\textsuperscript{164} Further, she ruled that the procedures for licensing encryption software constituted prior restraint on freedom of speech.\textsuperscript{165} Finally, on this basis she ruled that the Export Regulations were unconstitutional.\textsuperscript{166}

\textsuperscript{162} Karn, ibid., at 11.
\textsuperscript{163} The court rejected Karn’s appeal for another reason and that is that the Arms Export Control Act established that decisions taken by those authorized under that law were not subject to judicial review. Karn appealed against the judgment, but the appeals court returned the case to the court of first instance (107 F.3d 923). This was because of the fact that, prior to consideration of the appeal, authority for issuing regulations in regard to restricting export of encryption software was transferred from the Department of State to the Department of Commerce, and the latter was due to issue new regulations regarding that subject.
\textsuperscript{165} Bernstein v. United States Department of State, 945 F.Supp. 1279 (N.D. Cal. 1996).
\textsuperscript{166} Bernstein v. United States Department of State, 974 F.Supp. 1288 (N.D. Cal. 1997).
The United States Court of Appeals for the Ninth Circuit, in a three-judge panel, upheld the ruling issued by Judge Patel, but in a slightly more restrictive manner: the Export Administration Regulations were found to be unconstitutional, but not in an all-encompassing sense. Only when the Administration imposes a restriction that prevents the flow of scientific ideas (whether by means of source code or some other means) without distinguishing between those and encryption products as commodities, does there exist an unconstitutional restriction. That is, the court ruled that not every program can be considered expressive speech – only when “[c]ryptographers use source code to express their scientific ideas in [...] the same way that mathematicians use equations or economists use graphs” does the Constitution provide protection under the First Amendment. It is important to note that although the specific expression under discussion also includes a “non-speech element,” the court noted that the O’Brien ruling do not have to be applied in all cases such as this, and, in light of the prior restraint of freedom of speech, it applied the highest standard in examining the extent of First Amendment protection.

In response to this decision, the United States Justice Department petitioned the court for a rehearing in the Bernstein case by an expanded panel. This petition was granted by the court, which withdrew the ruling by the three-judge panel. However, changes in encryption export policy made the appeal hearing moot, and the case was returned to the District Court.

The third case dealing with the issue of encryption software and freedom of speech is the Junger case. Professor Peter Junger is a lecturer at Case Western Reserve University in Cleveland who teaches a course in “Computing and the Law.” Junger wrote a number of very basic encryption programs, and wanted to post them on the course’s Internet site, in order to show his students “how a computer works.” Since, under the International Traffic in Arms Regulations, or ITAR, cryptographic computer software is considered a “munition,” he was required to obtain an export license from the Department of Commerce. His application was refused, and so he

167 Bernstein v. United States Department of Justice, 176 F.3d 1132 (9th Cir. 1999).
168 Ibid., at 1141, 1145; Judge Nelson, in a minority ruling, held that computer software cannot be considered speech.
169 Bernstein v. United States Department of Justice, 192 F.3d 1308 (9th Cir. 1999).
170 15 C.F.R. § 734.2(b)(9).
appealed to the Federal District Court in Ohio, claiming that his First Amendment rights had been violated. The court accepted the position put by the government, and ruled that the export of cryptographic software is not protected by the First Amendment, even if encryption software occasionally includes a “speech” component. The reason for this is that software primarily provides functionality, and expression is only a secondary aspect. Junger appealed to the Court of Appeals for the Sixth Circuit, which rejected the decision of the lower court. In the appeal, the court ruled that the functional characteristics of source code do not overshadow its expressive nature, and that the O’Brien ruling should be applied in such cases.

In two other cases, known as the DVD judgments, the courts in New York and California ruled on the constitutionality of restrictions on the publication and dissemination of software to break digital protection mechanisms. Here, too, the courts were not of one mind in their judgments.

The factual background of the two cases is almost identical. The American film industry attempted to protect its investment in films in digital format on DVD by means of a technology called Contents Scramble System (CSS), which is designed to prevent unlicensed viewing of the film on the disk or of a copy. A Norwegian teenager wrote a program – DeCSS – that breaks this protection technology (according to the writer, with the aim of allowing the viewing of DVD films on drives operating under Linux). The code for the decryption program was disseminated to universities through the Internet, and the plaintiffs, who were interested in finding the most effective way of cutting off its distribution, decided to sue the operators of websites that distributed the code.

In the first case, which was heard in New York, the main defendant was a well-known hacker named Eric Corley, who placed a copy of the decryption program on his website. The film companies sued him on the basis of the explicit provisions of the Digital Millennium Copyright Act (DMCA), which prohibits the publication or distribution of software to break digital protection mechanisms. Judge Lewis A.

---

172 Junger v. Daley, United States Secretary of Commerce, 209 F.3d 481 (6th Cir. 2000).
Kaplan, sitting in the District Court, ruled in favor of the film companies. Corley appealed, but the appeal was rejected. One of Corley’s main arguments was that applying the DMCA to the distribution of the decryption program violated his constitutional rights to freedom of speech, since it had already been ruled that computer code is a protected speech under the First Amendment. Both courts agreed that computer code does constitute protected speech. Judge Jon O. Newman, in the Court of Appeals, even noted that this determination was valid, even though the code was comprehensible only to programmers, in exactly the same way that musical notes, comprehensible only to musicians, constitute protected speech. The extent of the protection, so it was ruled, is influenced by the fact of the program being a combination of a speech element and a functional, or non-speech, element, and therefore the appropriate standard to be applied is that of “intermediate scrutiny,” and not the absolute standard. In other words, the appropriate test to apply in this instance is the O’Brien test. Furthermore, it was ruled that the DMCA is not aimed at inhibiting freedom of speech, or the ideas embodied in the decryption software. Rather it is aimed at serving an important interest – one which is also constitutional – that of protecting copyright works and preventing “piracy.” Also, the limitation on freedom of speech imposed by the law is proportionate, since there is no other way of achieving its goal, and thus the DMCA prohibition on the distribution of DeCSS is, in fact, constitutionally valid.

Similar proceedings took place on the West Coast of the United States, in a suit submitted by the DVD Copy Control Association, the holder of the rights to the CSS system. DVD CCA licenses installation of the system to producers of DVD players. The suit named Andrew Bunner, who published the DeCSS program on his website, as defendant. However, the decision of the Californian court was fundamentally different from that of the courts in New York. This time, freedom of speech won. The lower court, issued, under the Uniform Trade Secret Act, an injunction against Bunner and others, ordering them not to publish or distribute DeCSS, on the grounds that the

175 Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2nd Cir. 2001) (Universal II).
176 Universal City, 111 F.Supp.2d, at 327.
177 Universal II, 273 F.3d, at 445.
178 Universal City, 111 F.Supp.2d, at 328-329.
180 Universal City, 111 F.Supp.2d, at 330-333.
decryption program contained CSS trade secrets. Bunner appealed to California’s Appellate Court, which overturned the original ruling. Again, the court held that computer code constitutes protected speech under the First Amendment, but in this instance the court did not adopt the O’Brien test, and permitted publication of the code. The reasoning was as follows: in determining the balance between freedom of speech and trade secrets protection, which is not a constitutional protection, the court applies the highest standard, and not the “intermediate scrutiny” standard that corresponds to the O’Brien test.\footnote{DVD Copy Control Association v. Bunner, 113 Cal. Rptr. 2d 338, 350-351.} It may be that the plaintiff’s strategy, which only made a trade secrets argument against the alleged freedom of speech violation, and did not present arguments based on copyright and DMCA infringement issues, is what undermined the claim.\footnote{Haim Ravia, “Pitzuah Ha-DVD [Cracking the DVD]” (18.11.01). available at: http://www.law.co.il/hebarticles/bunner.htm.}

Israeli courts have not as yet been asked to deal with this question. Freedom of speech is recognized in Israel as a fundamental principle, although it is an unenumerated right. In a number of decisions, the Supreme Court has ruled that this right is to be read into the Basic Law: Human Dignity and Liberty. Therefore, it may be assumed that the limitation on speech will be examined in light of the “near certainty” test, and this is likely to be read into the limitations clause.

5. Freedom of Occupation

The infringement of freedom of occupation

The legal regulation of encryption limits involvement in encryption. Thus, in evaluating this regulation or formulating any new arrangement, or when applying the existing arrangement, such regulation should be examined in light of the fundamental right to freedom of occupation, as established in the Basic Law: Freedom of Occupation.\footnote{Basic Law: Freedom of Occupation, 5744-1994, Sefer Hukkim, 5744, 90.}

The amended Control of Commodities and Services (Engagement in Means of Encryption) Declaration uses a broad definition of engagement, which includes, inter

\footnotesize
\begin{itemize}
\item \footnote{DVD Copy Control Association v. Bunner, 113 Cal. Rptr. 2d 338, 350-351.}
\item \footnote{Haim Ravia, “Pitzuah Ha-DVD [Cracking the DVD]” (18.11.01). available at: http://www.law.co.il/hebarticles/bunner.htm.}
\item \footnote{Basic Law: Freedom of Occupation, 5744-1994, Sefer Hukkim, 5744, 90.}
\end{itemize}
alia, “development, production, integration, acquisition, sale, use and export of means of encryption.” As stated in the Encryption Order, which implements this definition, “no person shall engage in the means of encryption except by license from the Director and in accordance with the conditions of that license.” In practice, upon commencing work with a new means of encryption, the applicant must submit an application for a license for all types of engagement, to the Supervisor of Military Export Controls in the Ministry of Defense, in order to receive a license to develop encryption measures. Later, when the applicant has a completed means of encryption, he needs to submit an additional application for a license for production, export, sale or any other necessary dealing.

In the case of completion of development, a change in the product, or a significant version change, he must submit, along with the application, a “working” version of the product, source code files, associated documentation and other materials that the Ministry may request. This is to allow a comprehensive examination of the product to be carried out. At the end of this examination, the applicant will be granted a suitable license or, as decided by the Director-General upon the recommendation of the advisory committee, sent notice of rejection of the application.

When a license’s expires, a company engaging in means of encryption is required to submit an application for license renewal. This application must be accompanied by a declaration that no changes have been made in the means of encryption. In cases of renewal of a license to sell the means of encryption, a report on the destination of sales must also be attached.

These procedures limit the freedom of occupation, which is established in a Basic Law. The Basic Law establishes explicitly that all governmental authorities are required to respect the freedom of occupation of every citizen or resident. The requirement that anyone interested in engaging in the means of encryption is required to apply for approval from the Director-General of the Ministry of Defense, casts a heavy shadow on the Ministry’s commitment, as a governmental authority, to respect the right of an individual to freedom of occupation. As noted previously, the policy

184 Ibid., Section 5.
adopted in practice by the Supervisor of Military Export Controls infringes less on freedom of occupation, but our recommendation is to close the gap between the practical policy and the legal authority. Therefore, it would be appropriate to examine the constitutionality of the existing regulations, and not to rely on the fact that present practice is less damaging.

Subordination of the existing arrangement to the Basic Law

The Control of Commodities and Services (Engagement in Means of Encryption) Order (Encryption Order) of 1974 was issued by the Minister of Defense under the Control of Commodities and Services Law, 5718-1957. Already in its original formulation, in 1974, a basic restriction on engaging in the means of encryption was imposed: “No person shall engage in the means of encryption except by license from the Director and in accordance with the conditions of that license.” There is no doubt that this is a legal provision that was in force prior to the enactment of the Basic Law, and thus, according to the text approved by the legislature, it remained valid until March 14, 2002.\(^\text{185}\) The Basic Law was enacted in 1992, quite some years after the Encryption Order was signed. As a result, there is a certain legal difficulty in treating the Encryption Order as void. However, according to the provisions of the provisional measures clause, the Encryption Order must be interpreted in the spirit of the provisions of the Basic Law: Freedom of Occupation.\(^\text{186}\)

At the same time, the Control of Commodities and Services (Engagement in Means of Encryption) (Amendment) Declaration published on August 13, 1998, does not benefit from the preservation of laws section in the Basic Law.\(^\text{187}\) This amendment contained a new definition of the terms “engagement in the means of encryption,” which did not limit the violation of freedom of occupation rights. To a certain extent, it even widened it. The amended Encryption Order, which was also issued on the

---

\(^{185}\) Ibid., Section 10.

\(^{186}\) In Supplementary Criminal Hearing 2316/95, Ganimat v. state of Israel, PD 49 (4), 589, 654, Chief Justice Barak writes: “What is the anatomy of the influence of Basic Laws on the interpretation of old law? Obviously the Basic Laws do not change the language of the old law… The only possible change can be in our understanding of it… The place for such change in the understanding of the old law is in the objective purpose of the item of legislation… In defining this objective purpose we often have to balance between conflicting basic values… And it is here that the Basic Law carries out its interpretative activity. By virtue of it a different weight may be given to the values and interests stated therein, than was given previously. As a result, the balance between those interests and values that determine the objective purpose of the law may change…”

\(^{187}\) Kovetz Takanot 5917.
same day, and, as we have said, makes use of the definitions contained in the Declaration, is not more lenient in the restrictions that it imposes. Rather, it makes the procedure for obtaining a license more complicated and less certain, since it divides the types of licenses into three classes, and appoints an advisory committee alongside the “Director,” to which he may delegate his authority for considering and deciding on license applications submitted to him. It may be that these amendments ought to be subject to judicial review, by virtue of their being provisions that impair freedom of occupation. Judicial review has been carried out by the Supreme Court in a number of cases, regarding legal provisions that stood in contradiction to the rights anchored in the framework of the constitutional revolution.\footnote{188}

It has been determined that “the remedy for the unconstitutionality of the law is its annulment, and the authority for determining that unconstitutionality is given to the courts.”\footnote{189} The right to judicial review, in the context of examining whether legislation is valid or void, is based in the Violation of Freedom clause in Section 4 of the Basic Law: Freedom of Occupation.

Firstly we need to address the question of whether the fact that the limitation in our case is created by an “Order,” which is quite low in the hierarchy of subordinate legislation, ignores the requirement that any limitation on a basic right be done by means of a law. It would appear that this distinction is not critical, given the rider in Section 4, “or by such a law enacted with explicit authorization therein.” The Order was issued by the Minister of Defense by virtue of the authority granted in the Control of Commodities and Services Law, 5718-1957.\footnote{190}

Furthermore, it appears that the issue of the Encryption Order according with the values of the State of Israel and having proper purpose is also not problematic. It is reasonable to suggest that national security is an appropriate value that constitutes a proper purpose for regulating engagement in the means of encryption. The problem

\footnote{188 See for example BGZ 1715/97 \textit{Lishkat Menahalei HaHashkaot BeYisrael} v. Minister of Finance, \textit{PD} 54 (4) 367; BGZ 6055/95 \textit{Sagi Zemach} v. Minister of Defense \textit{Tak. Supr.} 97 (4), 140; Civil Appeals 6821/93 \textit{Bank Hamizrachi v. Migdal}, \textit{PD} 49 (4) 221 (below: the Bank Hamizrachi case); BGZ 1031/99, 1030, 1053, 1119, 1201 \textit{Cable et al. v. Speaker of the Knesset et al.} (not yet published).}

\footnote{189 See Bank Hamizrachi case, ibid., at p. 418 (Justice Cheshin).}

\footnote{190 \textit{Sefer Hukkim}, 5718, p. 24.}
arises in regard to the question of proportionality. Former Chief Justice Shamgar established, in the Bank Mizrachi case, three cumulative tests for determining the proportionality of such a violation of rights: appropriateness for achieving the purpose, minimization of the violation, and reasonableness of the violation.\(^1\)

**It goes without saying that primary legislation or amendment to existing subordinate legislation today needs to meet the conditions of the limitation clause in the Basic Law: Freedom of Occupation.**

The main question in this regard is that of proportionality, and this in turn arises from one of the key characteristics of encryption products. Encryption products are dual use products: they can serve constructive civilian ends, such as providing protection for personal information or commercial data, yet they may also serve as a weapon in the hands of terrorists.

Therefore, we believe that, in order to meet the requirements of proportionality, any system of regulation needs to be based on the characteristics of the products in question, and the functions they are supposed to fulfill.

- It would be appropriate to distinguish, as much as possible, between different uses for encryption products. The existence of a range of situations should be recognized. At one end of the spectrum would be products that are used solely for commercial use, and have no defense applications at all. At the other end would be those products that are purely defense-oriented, with no civilian uses. It is clear that the bulk of products would be spread along this range, and where exactly they lie would have to be determined by the courts.

- Products located or leaning toward the civilian end of the spectrum, should be totally exempt from regulation. This would include, for example, products for verification of digital signatures.\(^2\)

- On the other hand, there is no problem with the regulation of products at the other end of the spectrum, those with a defense or security orientation.

---

\(^1\) See Bank Hamizrachi case, supra note 189, at 347 (Chief Justice Shamgar).

\(^2\) This already exists to a certain extent, with certain means of encryption being defined as “free means.” However, the number of encryption products currently classified as free is limited, and thus arises the problem of a lack of proportionality.
As for the variety of products in the middle of the range, proportionality can be achieved by providing clearer definitions of what is permitted and forbidden, by delineating more clearly the authority’s discretion, and by the existence of judicial review.

In addition, the system of regulation has to explicitly distinguish between the aims of the producer of encryption products.

- Products which, by their nature, are for private uses only should not be subject to any form of regulation. Therefore, the marketing of such products on the local market should be exempt from regulation.
- In order to achieve the security goals, limitations may be applied to the export of those products whose uses place them closer to the defense end of the spectrum.

6. Property Rights

Regulation of encryption also has impact on property rights, which enjoy explicit constitutional status.\(^{193}\) The main impact is caused by the procedures required to be followed by a license applicant.\(^{194}\) Here, too, the policy adopted in practice by the Supervisor of Military Export Controls is less offensive than what would be implied by the broad authority found in the subordinate legislation. However, in our view, not only should the practical policy be constitutionally valid, but also its legal framework. As we have noted, we feel that the legislative framework and the policy in practice need to be brought into line with each other. The Order requires the provision of the program itself as well as associated materials, for examination prior to approval by the authority – in this case, the Ministry of Defense. In practice, this requires the provision of source code files and disclosure of the algorithm used by that encryption product. The Defense Ministry claims that, in practice, only a small proportion of companies is asked to divulge the source code.\(^{195}\) However, since companies do not know ahead of time whether they will be asked to divulge their algorithms, this creates a “chilling effect,” in addition to the obvious damage done to those companies

\(^{193}\) Basic Law: Human Dignity and Liberty, Section 3.
\(^{194}\) Control of Commodities and Services (Engagement in Means of Encryption) Order, 5735-1974 (“the Order”), Section 2.
\(^{195}\) See Yoram Cohen’s comments at the Shefayim Conference.
that are required to divulge their source code. In terms of proprietary concepts, this is a forced disclosure of trade secrets. Trade secrets, however, are protected under the law, both in legislation and in judicial rulings.196

As in our discussion of the right of freedom of occupation, here, too, the existing system of regulation, and certainly any future system of regulation, are subject to constitutional review. Also, as in that discussion, property rights are not absolute, and may be violated under the terms of the limitations clause.

Therefore, we believe that an explicit definition of the licensing process, along with a clear statement that the State may not violate the applicant’s trade secrets, should answer the requirement of proportionality. It might also be possible to add an obligation on behalf of the State to composite the owners for any violation of these obligations.

F. Summary of Recommendations

1. The regulation of encryption by means of subordinate legislation, in the framework of economic law, is in appropriate. By its nature this is a primary arrangement, that has implications on basic human rights. In practice, the policy that has been adopted establishes prohibitions and permissions without specific legislative authority, and thus the determination of policy is carried out by the executive branch without the direction of the legislator. This situation is not desirable from the point of view of the principles of administrative and constitutional law, and has negative implications for the flexibility of the policy adopted in practice, such as the chilling effect that it has on the industry.

Therefore, we believe that the legal response to encryption needs to be established in primary legislation.

196 See Commercial Wrongs Law, 5759-1999; BGZ 1683/93 Yavin Plast Ltd. v. National Labor Court, PD 48 (2) 244.
2. The aim of the legislation is to answer real security needs: safeguarding security and other sensitive information, and protecting surveillance and intelligence gathering measures used by the defense and security establishment. These needs are not superfluous, in spite of the high accessibility and availability of encryption products. Therefore, this legislation has a worthwhile purpose, and is in line with the values of the State of Israel, as required under the Basic Laws.

3. The existing system of regulation and the proposed legislation impinge negatively on freedom of occupation and property rights, and may violate the right to privacy and threaten the right of freedom of speech and academic research. Therefore the present system of regulation ought to be interpreted in the spirit of the Basic Law, and the proposed legislation needs to meet the proportionality test in the Basic Law: Freedom of Occupation and the Basic Law: Human Dignity and Liberty.

4. In order to meet the proportionality test, the law must define, clearly and explicitly, the scope of the regulation, its tests and the extent of the Authority’s discretion.

5. A number of models exist for regulation. We believe that the clock cannot be turned back, and that it is inappropriate to adopt a model based on a sweeping prohibition accompanied by specific exclusions. The existing legal model is one of prior licensing, and it is with this that we shall deal first.

The Licensing Model:

6. The extent of the Authority’s discretion needs to be defined, and limited to actual security needs. Among these, the need to prevent terrorist activity, as opposed to the need to obtain evidence after the fact, ought to receive priority.

7. Those areas of activity that require prior licensing need to be defined. To this end, it is necessary to distinguish between private/civilian uses and defense/security uses. Those uses falling in the first category ought to be exempt from any form of regulation. Where it is more difficult to classify a product as
purely or mainly private/civilian, due to the dual use nature of encryption products, regulation becomes appropriate, subject to the following:

8. **The aims of the producer should be identified**, and the requirement for licensing should be limited to only a portion thereof. In particular, distinction should be made between local marketing and export. Given that security needs include the need to make it harder for terror organizations to acquire encryption products, it is appropriate to institute export controls. Control of local marketing, on the other hand, is less justified, particularly when the product’s purpose is closer to the civilian end of the spectrum.

9. **Criteria for control need to be explicitly defined**: Have the product’s final destination or encryption power been checked? Different countries adopt various tests. We have no definite opinion regarding the appropriate test to adopt, but simply state that criteria need to be established, so that industry can plan accordingly and operate with a higher level of confidence.

10. **The approval process needs to be defined explicitly**:
   - The amount and types of information that the Authority is entitled to request of a producer applying for a license must be limited;
   - The process stages for examining applications must be fixed in law; details of the examination process may be fixed in the subordinate regulations;
   - An appeals process for applicants whose request has been denied needs to be established. It may be that the appropriate place for this is in the judicial review function of the Administrative Affairs Court, in the form of an administrative petition. In this case, special procedures ought to be established to ensure the secrecy of proceedings.

11. **Decryption**: In those cases where the relevant Authority requests access to an existing encryption product, that is, via a “back door,” a suitable mechanism for prior judicial review needs to be created, similar to that adopted under the Secret Wiretap Act, 5739-1979.
Registration Model:

12. Alternative models for regulation ought to be considered. One possible model is that of registering encryption products without imposing prior control on them. Such a model, similar to the registration of databases under the Privacy Protection Law, 5741-1981, will impose one single obligation on the producers of an encryption product: the registration of its existence and the provision of general information about the product. By this means, the Authority can know which products are in whose hands. Where necessary, the Authority may apply to the courts for permission to penetrate the encryption product.
III. Online Monitoring: Security, Privacy and Freedom of Speech

A. Introduction

In recent years the Internet has become a primary medium for message transmission and information management. The Internet furnishes facilities for sending and receiving messages between different agencies and for managing information efficiently, accessibly and interactively. The technological developments and the information age have had a major influence on the thinking and methods of work of intelligence organizations worldwide. While the classical intelligence source was principally Human Intelligence, the intelligence organizations have lately begun to base their work on obtaining intelligence through technological means and primarily through SIGINT – Signal Intelligence. SIGINT means intelligence produced by listening to and decrypting signals, whether in electromagnetic waves or fiber-optic transmission and any other communications standard, including data communications and Internet. For instance: e-mail, instant messages and site infrastructures. The changed outlook and the transfer of emphasis to technological intelligence derives inter alia from the fact that the intelligence targets use various and diversified communications means and are therefore far more exposed than in the past to monitoring by those means. Alongside the legal activity on the Web (such as e-commerce, education and teaching, academic research), the Internet also serves as a communications means for intelligence targets of various kinds: from criminal agencies to terror organizations. Given its centrality as a means of communication, the Internet is naturally an important target, constituting a source of intelligence material collection for the intelligence organizations.

---


198 Human Intelligence – HUMINT. Namely intelligence derived from human collections sources, for instance: spies, agents, collaborators, interrogation of captives. In the past, this was the exclusive and most qualitative intelligence source. It is still in use today, although alongside additional sources produced by other non-human means.

199 Signal Intelligence (SIGINT) refers to communications intelligence, electronic intelligence, technological intelligence. It involves principally wiretapping on telephone, cellular and fax communications, and in recent years also the Internet, e-mail. Sometimes, as a preliminary stage for producing the finished product, the encryption means protecting the source must be cracked. SIGINT today constitutes the most widespread and quality intelligence means, in particular among the leading intelligence organizations in the world, that have the most sophisticated technological infrastructures.
Use of the information environment in online monitoring gives the intelligence organizations several salient advantages in information collection. Firstly, in the past, collection of intelligence material called for investment of tremendous resources and manpower or was completely impossible. Electronic monitoring means, working on a global web, together with very powerful computer capacities, allow efficient collection of such material. Secondly, any action in a digital web leaves “digital tracks”. The routine operations of sending electronic mail, surfing, sending and downloading files, in fact constitute data processing and are recorded in various files of the PC and the servers involved in the communications. For instance, unlike a telephone call that remains in space and in the memory of the speakers only, a chat room discussion creates details of the contents, and also of the date on which the message exchange was conducted, the computers and servers through which it was executed, etc. In addition, the Internet allows transfer of complex message in different formats: not only text exchange by e-mail, but also chat in real-time, speech, video pictures, and of course also computer software and applications. In these circumstances, the wealth of information that can be collected, and the level of detail are unprecedented.

However, the advantages of the information environment for information monitoring and collection are liable to create a new kind of threat to individual liberties, since the means of information collection and monitoring in this environment are more invasive and state-of-the-art, and also because of the form of monitoring required in light of the unique characteristics of Internet communications. For instance, Internet communications are based on distribution of data to “packets” sent by the sending computer and routed in the Web separately, until finally they are collected and arranged by the receiving computer. In these circumstances, transmissions of intelligence targets are liable to be swallowed up in innocent transmissions. Therefore monitoring of the Internet involves, in many cases, monitoring and collection of extensive material also on people who are entirely innocent.

Given the unique characteristics of the Internet, it may be necessary to reexamine the existing regulations expressing the checks and balances between wiretapping for security needs and the rights of the individual. Legislation in democratic regimes
strikes a balance between the intelligence needs of the various security authorities and safeguarding the rights of the individual. The application of the existing checks and balances in the digital environment might call for adjustment to needs, means and the new threat to the rights of the individual. Further, the legal analysis must take into account the fact that many intelligence operations are liable to be carried out on equipment and servers of commercial agencies, and at times even through them.

This chapter discusses the question of the most appropriate legal framework for intelligence activities on the Internet. The discussion will commence with a short review of the characteristics specific to the monitoring means and the intelligence collection activities in the information era. We will then discuss the threats that these means are liable to pose to the rights of the individual, such as the right to privacy and free speech. Finally, we will review the existing checks and balances between the intelligence needs and the rights of the individual in the framework of the existing legal regulations. We will examine to what extent the existing legal framework provides a response to the security needs in the digital environment, while simultaneously providing sufficient protection for the rights of the individual.

B. Intelligence in the Information Age

1. General Background

There are three stages to intelligence work in the information age. In a first stage, an intelligence organization must identify the technological infrastructure that it wishes to penetrate. Sometimes this is extremely simple, and can be carried out by the average intelligent person. For instance: interception of an analog communications network that can be received by a simple radio. Sometimes, a complex extremely difficult task is involved, that might demand development of a system for receiving and interception of the said broadcast, sometimes even with cracking of sophisticated security. For instance: encrypted on-line communications or hacking into computers.

---

200 Article 13 of the Bezeq Law, 5742-1982, orders allocation of resources, in pursuance of the decision of the Minister of Defense or the Minister of Internal Security, by a licensee for carrying out of Bezeq activities, for provision of Bezeq services or satellite transmissions, for the security forces. The license for carrying out of Bezeq services also comports special articles, setting down specific instructions in relation to the licensee’s obligation towards the defense system. For instance, CellCom’s Adv. Sharon Keren in his lecture noted that Article 48 of CellCom’s license orders the outright allocation of resources to the Defense System. Section 66a of the CellCom license obliges the company to allocate special services to the Defense System.
protected by a Firewall. **In the next stage**, the intelligence agency must intercept the transmission and in fact listen in to it. This requires manpower that must be able to handle transmission in different languages, reading of texts etc. At times, and in light of the tremendous quantity of information, a computerized platform serves in this role, operating algorithms that can, for instance, identify, suspicious words in a text or speech. Therefore, filtering is a critical element in intelligence work, and as will be seen subsequently, it characterizes modern intelligence agencies in their current war on terror. **The third and last stage** is analysis, research and distribution of a finished intelligence product to the intelligence consumers from relevant low echelons to leaders of states. This stage is less relevant to the current discussion. These stages can be demonstrated through the activity of the NSA, which will be described below.

Intelligence agency activity is, not surprisingly, secret. Accordingly any information in this regard can be obtained only indirectly and partially from articles published in the media on this activity and the means employed. Journalistic sources,\(^{201}\) and different human rights organizations that monitor the activity of intelligence agencies,\(^{202}\) report that the largest intelligence agency in the world in the SIGINT area is the American **NSA: National Security Agency**. This organization works alongside the CIA and the FBI and has an equal status with them as a federal agency. It is also maintained that the USA, in conjunction with other Western countries, operates a technological system that allows real-time interception of messages transmitted through many communications means worldwide. This is an international spy and wiretapping network called **Echelon**, which is operated by the NSA, in conjunction with the intelligence services of Canada, Great Britain, Australia and New Zealand. The original project was created in 1971, but its spheres of activity have gradually expanded since then.\(^{203}\) According to the ACLU report, “Echelon” is installed today in some one hundred and twenty wiretapping stations deployed in Seattle, West Virginia, Puerto Rico, Denmark, New Zealand, Canada, Australia, Holland and


\(^{202}\) See for instance the Echelon Watch of ACLU (the American Civil Liberties Union), at - [http://www.aclu.org/echelonwatch](http://www.aclu.org/echelonwatch).

\(^{203}\) The project was founded in pursuance of the UKUSA Signals Intelligence Treaty 1948. Even though this is a secret treaty, references to it can be found in various Internet sources, including also highly credible sources. See for instance the reference to the treaty at the site of the Federation of American Scientists at: [http://www.fas.org/irp/eprint/sp/sp_f2.htm](http://www.fas.org/irp/eprint/sp/sp_f2.htm).
Cyprus, and uses satellites. The US has never officially admitted the existence of the system, but a European Union committee set up to investigate the subject of “Echelon” recently determined that the electronic spy network exists and even provided proofs of its existence.

The Echelon Project has a secret monitoring system installed in super-computers that can receive three billion electronic transmissions daily (according to estimates, approximately ten billion messages pass through the Internet daily). The report of the European Union committee for investigation of ECHELON, which was approved by the European parliament, strengthened suspicions that “ECHELON” can receive and intercept communications of surfers around the world: telephone calls, faxes, satellite communications, e-mail, downloading of software from the Internet, microwave communications and fiber-optic transmission. Mainly, ECHELON does not record calls but “monitors” the system. For this, it uses Sniffer software programs that control the information transmission on six main backbones in the Internet, and collect as much information as possible, which is then transferred to a “dictionary”, a collection of artificial intelligence software programs specializing in locating material of intelligence value. ECHELON software locates messages containing suspicious words (e.g.: “explosives”, “Bin Laden”, “al-Qaida”, and seemingly innocent code words, known among the intelligence agencies as characterizing intelligence targets), intercepts them, classifies them and sends them to the intelligence arms in the different countries.

2. Means of Collecting Information and Monitoring the Internet

For purposes of the legal discussion, the different Internet monitoring means can be classified according to the way in which the information is collected: by monitoring, namely recording operations carried out on the communications network by various

---

204 See the list of “suspected” listening stations, based on newspaper sources, experts in the field and books on the subject at the Federation of American Scientists site: http://www.fas.org/irp/news/1999/02/radome.htm

205 Report on the existence of a global system for the interception of private and commercial communications (ECHELON interception system) - Temporary Committee on the ECHELON Interception System. See: http://www2.europarl.eu.int/omk/OM-Europarl?PROG=REPORT&L=EN&PUBREF=-//EP//TEXT+REPORT+A5-2001-0264+0+NOT+SGML+V0//EN&LEVEL=2

206 A Sniffer is software that “passes” over a main Internet server or telephone switchboard and examines all its activity according to various parameters. Relevant communications activity is “retrieved” and transferred for continued intelligence handling.
users, or by hacking into the computer server and recording the activities carried out on the server. The distinction between monitoring operations in the public sector and monitoring operations in the private sector (hacking into sectors that are the user’s private property) is liable to have legal ramifications. Another aspect likely to have implications for the legal analysis is the type of information collected: for instance, the communications contents, the communications log only, or general/statistical demographic date on user groups in the system.

2.1 Information Monitoring

Information monitoring in fact constitutes state-of-the-art wiretapping through a Sniffer, software that scans the service provider and examines its entire activity according to different parameters. The most well-known and widely publicized Sniffer of late is the Carnivore.207 Officially, the Carnivore was designed to fight crime – pedophilia for instance. However it naturally becomes a relevant and practical tool also for fighting terrorist organizations, which make frequent use of the Internet.

Monitoring of Internet transmissions is carried out in general passively; the system monitors all the communications and extracts, while recording, the specific information in which it is interested (identification of the relevant packets). In the past, it was claimed that the system is active, and itself plants information in the transmission, in order to render its activity more efficient. However, as far as is known, this is untrue. The monitoring in practice is carried out on the Internet providers’ systems. The intelligence material collected by Carnivore is identical in many cases to the information recorded in any case on the ISP’s as an integral part of operation of the Internet. In the legal situation existing prior to September 11, 2001, a search warrant was required in order for this information to be transmitted to the investigation authorities. This situation changed following promulgation of the USA PATRIOT ACT.208 When the FBI collects the information independently, the Sniffer is planted in an addressable branch box by the FBI on the ISP information nodes. American ISP’s have reported that even prior to September 11 the FBI tried to bribe

---

207 This name was given to the software by the FBI since it “chews” all the information, but “swallows” and “digests” only the specific information desired. Recently the FBI rechristened it DCS1000 in a public relations campaign, since the actual name aroused criticism and violent public opposition. See the report at the ACLU site: [http://www.aclu.org/news/2001/w021401b.html](http://www.aclu.org/news/2001/w021401b.html). See Chapter IV-4 below.
them to install Sniffer software on the systems that they operate. Several ISP’s\textsuperscript{209} and naturally the human rights organizations\textsuperscript{210} campaigned against this. The resistance to Carnivore became less vociferous following the events of September 11. However, the ISP’s still voiced some protests in the matter, particularly following the new legislation.\textsuperscript{211}

Carnivore has two uses: content wiretap and identification of users.\textsuperscript{212} Content \textbf{wiretap} includes listening to electromagnetic or fiber-optic signals “broadcast” by the intelligence target, and filtering of the Internet communications from them, like telephone wiretapping. Generally e-mail messages sent from and to the intelligence target will be intercepted: technical traffic, activity in the e-mail account, or all the incoming and outgoing traffic of a specific user, or a specific IP address. Such a use requires federal court authorization.\textsuperscript{213}

Another use of Carnivore is for purposes of identifying the correspondents (\textbf{trap and trace} / \textbf{pen register}) and it includes location and identification of all those who contact or are contacted by the intelligence target. Said location and identification include: identification of e-mail addresses, identification of servers (Web, FTP) to which the intelligence target has access, monitoring the users of an Internet page or specific FTP, all the internet pages or FTP directories to which the target has access. The use of software for identification of correspondents without disclosing of the contents of the correspondence is widespread, and the legal limitations on this use are negligible.\textsuperscript{214}

\textsuperscript{209} See report on the ISPs’ fight, for instance: Mci, EarthLink, AOL versus the FBI, in conjunction with the ACLU, in the Wall Street Journal of 14.7.2000. A report on the WSJ article can be found at ZDNET: \url{http://www.zdnet.com/zdnn/stories/news/0,4586,2656409,00.html}

\textsuperscript{210} See for instance a letter from the ACLU on the subject of Carnivore to the members of Congress dated 11.7.200, at the ACLU site: \url{http://www.aclu.org/congress/107110a.html}.

\textsuperscript{211} See: “IT Workers Chew Over ‘Carnivore’ Bill” at the CNN site: \url{http://www.cnn.com/2001/TECH/industry/10/11/carnivore.resistance.idg}, and the continued public struggle conducted by the ACLU under the name: “Safe and Free in Times of Crisis” at the ACLU site: \url{http://www.aclu.org/safeandfree/index.html}.

\textsuperscript{212} The following technical information is based on Internet sources of varying levels of reliability, given the secrecy surrounding Carnivore. For instance: \url{http://stopcarnivore.org} and \url{http://www.robertgraham.com/pubs/carnivore-faq.html}.

\textsuperscript{213} See Chapter IV-4 below.

\textsuperscript{214} See Chapter IV-4 below.
With regard to e-mail, Carnivore in fact monitors the exchange of information between two e-mail users, one of whom is the target. The Sniffer’s primary interest is in the SMTP protocol created in this communication and which specifies the sender’s address, the addressee and the actual message made up of a **Header** and a **Body**. If the FBI has been authorized only to use **trap and trace** monitoring, then it is entitled to “listen” only to the first part of the protocol, containing details of the sender and addressee only.

The first part of the protocol is made up of data revealing the identity of the parties to the specific e-mail message:

```
<-220 mx.altivore.com SMTP server.
>>>HELO mx.example.com
<-250 mx.altivore.com Hello [192.0.2.183], pleased to meet you
>>MAIL FROM: <alice@example.com>
<-250 <alice@example.com> … Sender ok
>>>RCPT TO: <bob@altivore.com>
<-250 <bob@altivore.com>
>>>DATA
<-354 Start mail input; end with <CRLF>.<CRLF>
>>>(e-mail message)
>>>\n\n<-250 Queued mail for delivery
>>>QUIT
<-221 mx.altivore.com closing connection
```

The second part of the protocol is made up of a header and the body of the specific e-mail message:
It should be noted that in comparison with the “ECHELON” project, Carnivore is a “surgical” Sniffer only. It cannot and does not purport, apparently, to monitor large-scale traffic from a large number of users. This would seem to be, also, one of the reasons for the surprising “openness” displayed by the FBI as regards information on the Sniffer, its capacities and its method of use. However, even if the intelligence agency’s intention is to monitor the Internet traffic and e-mail of only one person, communications and computer agencies and artificial intelligence experts argue that the likelihood that the FBI will succeed “physically” in focusing on one person, or more precisely a single signal or byte, is almost zero, and therefore it is quite possible that there in an invasion of privacy of many other users in the target’s entourage.

2.2. Collection of Information on the Server or the PC

There are several hacking means planted in the PC for information collection. The most widespread commercial means is the use of the technology called Cookies. This is a text file, stored by the site on the surfer’s hard disk, which allows recording and monitoring of the user’s surfing habits, e.g.: the sites that the surfer visited, the advertisements displayed to him and whether he answered them, and so forth. Originally the cookies were designed to obviate the inconvenience of repeat registration to sites that made use of them conditional on delivering of personal details. Technically, planting of the file does not require the user’s knowledge, agreement or cooperation. Nonetheless, in the new versions of browsers, it is possible
to cancel receipt of cookies, to change the browser definitions so that it will warn the
user every time that a site tries to send him a cookie, or to delete the cookies in the PC
after each Internet connection.215

It should be noted that this technology does not in itself allow collecting of
information on the surfer, his identification by name or his physical address. However
the surfer frequently himself delivers this information or defines it in the browser, and
sometimes these details can be derived from cross-referencing of a few databanks.
The commercial use of cookies raises serious questions concerning protection of
privacy, and this matter has been discussed frequently by the European Union.216

The Magic Lantern System

Another means that made the headlines and was subjected to public debate, after
September 11, was Magic Lantern. This is a system used by the FBI for handling of
encrypted information on the computers of criminals and terrorists.217 While
information monitoring through Sniffers such as Carnivore has its advantages for the
information-collecting agency, the difficulty of deciphering encrypted material that
was collected still remains. The Magic Lantern solves this difficulty for the
intelligence agency, crossing another line and arousing concern for the privacy of
individuals and organizations.

215 Programs that delete cookies provide a more efficacious solution against cookies. Software such as
Guidescop and Burnt Cookies monitor the changes in the directory where the cookies are stored.
Through them it is possible to delete cookies, to peruse the cookies on the hard disk and to decide
whether to save them or delete them. The review is based on Gal Mor, “Ro’im Lanu et Hakol” (They
can see everything) at: www.ynet.co.il/Ext/Comp/ArticleLayout/CdaArticlePrintPreview/1.25061.
234131.00.html. See also the site: www.cookiecentral.com and Haim Ravia, “Al Glisha u-Pratiut – o al
Ugiyot Bareshet” (On surfing and PRIVACY – or on Cookies on the Internet) at:
protection of individuals with regard to the processing of personal data and on the free movement of
such data. The text of the directive can be found at:
217 The Magic Lantern was first revealed in the press on 20.11.01 on the MSNBC communications
network site: http://www.msnbc.com/news/660096.asp. The intelligence agency publicly admitted the
use of Magic Lantern after media pressure only on 12.12.01. See the report on the MSNBC network
site: http://www.msnbc.com/news/671981.asp?bsi=-.-. The FBI’s first use of the software was in a Mafia
affair known as the Scarfo Affair. See the newspaper report on this affair at the Acnews.com site:
http://abcnews.go.com/sections/scitech/CuttingEdge/cuttingedge011221.html. FBI assistant
director Randall Myrch admitted to the court that, when monitoring Nicodemo Scarfo, a mafia leader in the
State of New Jersey, FBI agents had broken into Scarfo’s office and planted the software in his
computer in order to steal the encryption keys. These keys allowed the FBI to decipher encrypted
messages that served as criminal evidence against Scarfo.
The Magic Lantern is in fact keylogging software planted in the target’s computer. The software can “see” the passwords keyed in by the suspect and thus in fact reveals the encryption key that he uses. This results in simple and rapid deciphering of all encrypted material, from e-mail messages to credit card numbers. In order to plant the software, the FBI raises its hacking threshold to the privacy of the suspect in an unprecedented manner. The software is in fact a virus that can be sent to the target by e-mail or by a third party considered reliable by the target. The virus can be inserted virtually in the target computer also through other computer hacking means, and naturally the possibility of completely physical planting, involving a break-in, is not excluded.218

When the software is present in the target’s computer, the computer user is in fact in passive surveillance. The surveillance becomes active when the popular encryption application PGP (Pretty Good Privacy) in which the user must deliver a passphrase is operated, and he thereby in fact delivers to the surveillance agent the encryption key. It should be remembered that while the required content is protected by those keys, the actual keys are protected only by the password. The stolen keys naturally allow the holder the possibility of decrypting, while the user is convinced that the keys are in his possession only.

The public debate naturally focused on the question of privacy but also raised the interesting argument as regards the legitimacy of government activity containing elements considered criminal, in other circumstances, by hackers for instance.219 The use of the software also raises the question of handling of the “legitimate” virus by the various anti-virus companies. The FBI naturally attempts to persuade the companies to cooperate with it and not to “identify” the software as a virus, and there were even rumors of cooperation agreements between certain companies and the American government.220

218 As was the case in the Scarfo Affair.
219 See David Sobel, legal adviser of the Electronic Privacy Information Center) and Republican Senator Dick Armey at the MSNBC site: http://www.msnbc.com/news/660096.asp.
220 Network Associates (www.nai.com), the manufacturer of PGP and the popular McAfee anti-virus software, was accused of some kind of agreement of this kind. See the report on the affair and the company’s denial at Wired.com: http://www.wired.com/news/conflict/0,2100,48648,00.html Robert Graham, the well-known computer security expert in Internet circles, writes on his private site www.robertgraham.com: “The official company position of any mainstream company is that they have
C. Prevention and Enforcement in the Information Age and human rights

1. Foreword

Prevention and enforcement systems are the applied expression of safeguarding the public interest in general and public order in particular. As understood today, it is the government authorities that are entrusted with protecting the public interest by various systems for identification, interception and monitoring of information, in order to prevent activities that conflict with the public interest and including, of course, terror acts. The main danger in operation of monitoring and information collection systems is that they might prejudice the rights of the individual, in particular the right to privacy and freedom of speech.

The technological means available in the free information age have brought the discussion of the right to privacy to new areas. In order to invade a person’s privacy it is no longer necessary to conduct a physical search in his home. Today, invasion of privacy can be effected remotely by the press of a button. There are cases in which the actual government asks to set up permanent or temporary wiretapping means in the name of the public interest. Assuming that these means do serve the public interest, should there be an encroachment on the privacy of those innocent people who chanced to be in the path of the government in its search for the relevant information?

2. What is privacy and what is the right to privacy?

The roots of the right to privacy go back to early human history. Clear anchors exist in the Bible, in Greek mythology and in ancient China. In Western culture we can find roots as far back as 1361 in England, and 1890 in the famous article of Warrant and Brandeis who coined the phrase “the right to be left alone”. The right to data privacy is a relatively new right whose meaning is controversial. The difficulty of defining the right to privacy is well reflected in its definition as “an individual right

no position. It would be bad business to help law enforcement invade customer’s privacy, and it would be bad business to specifically work against the efforts of legitimate law enforcement. They are going to do their best to do neither.” At: http://www.robertgraham.com/journal/020110-magic-lantern-position.html.

that is self-evident until someone takes it away.” This negative definition is insufficient and the basic question is what “privacy” means. The term privacy describes a state of affairs, circumstances in which the individual is in relation to others. Therefore, \textit{the right to privacy} concerns those situations in which the law protects the right of the individual to protect his privacy. In American law the right to data privacy developed in the wake of the famous article by Warren and Brandeis, who argued that the right to privacy is a separate right, independent of other rights. Others such as William Prosser, argued that this right is made up of four causes of torts: intrusion upon the seclusion of another; appropriation of the other’s name or likeness; publishing of personal information and publicity that places a man in a false light. Over the years many attempts were made to define privacy and the right to privacy.

There are those who define privacy in terms of access. Namely, privacy relates to the individual’s ability to limit access to him. Ruth Gavison, for instance, argues that “Privacy is a limitation of others’ access to an individual.” In this sense, a loss of privacy occurs when others have information on the individual, when they draw attention to him, or receive access to him.

Others define privacy in terms of control. If in the past privacy concerned control in the individual-intimate space - “a man’s home is his castle”, then in the modern age this concept has been expanded and also applies to control of information about the individual or personal information. Therefore, privacy in the modern era means not only a man’s control of his physical private space, but also control of his intimate

---

(2) The right of privacy is invaded by:
(a) unreasonable intrusion upon the seclusion of another, ...; or
(b) appropriation of the other’s name or likeness, ...; or
(c) unreasonable publicity given to the other’s private life, ...; or
(d) publicity that unreasonably places the other in a false light before the public, ...
decisions, control of the knowledge of his personal affairs, or control of information about him. In this sense a man’s privacy is gauged by his ability to determine when, how, and to what extent use will be made of information about him. According to this approach, the right to privacy is a man’s right to control information concerning him, and the use of the information collected about him. A man is entitled to determine in what circumstances information about him will become public, i.e., will be published, or will be accessible to the general public in another way. This definition, naturally, necessitates a decision as to what private information is entitled to protection, and what rights of control the individual has in relation to this information. Since the right to privacy defines the border between the “private” (which must be under the individual’s control) and the “public” (which is outside the individual’s area of control), this right in many cases will reflect the social and cultural perceptions regarding distinction between private and public. The right to privacy, in the sense of a man’s right to control information about him, is liable to create a conceptual difficulty, since protection of data privacy in many cases calls for protection of “privacy” in what is defined as the “public domain”.

3. Is protection of privacy on-line justified?

The absence of a clear theoretical basis for protection of data privacy in the public domain may well be the reason for the vagueness of the legal definitions with regard to the right to privacy. In order for it be possible to define the nature and scope of application of the right to data privacy, it is necessary to examine the justifications for the existence of this privacy. Some view privacy as an independent value that should be protected, while others consider that privacy is not a value at all, or realistically argue that privacy is a thing of the past and is not sustainable in the modern electronic

---

228 Thus for instance Charles Fried considers that privacy is not only the other’s absence of information about us, but also our ability to control information about us. See: Charles Fried, “Privacy [A Moral Analysis]” in Philosophical Dimensions of Privacy, supra note 226, at 210 (1984); Charles Fried, “Privacy”, 77 Yale L.J. 475, 482 (1968).
231 On the vagueness of the definitions see: Gregory J. Walters, Human Rights in the Information Age A Philosophical Analysis (Toronto, 2001) at 158.
urban world. On the other hand, there are those who see privacy as a means designed to guarantee the existence and advancement of other values. There are several arguments as regards restriction of the State’s power in this context:

3.1 **Autonomy** Some stress the importance of the right to privacy as part of the limitations applying to the State in relation to the individual and designed to protect his freedom. In the broader context, this argument is liable to justify protection of the right to privacy not only in relations between citizen and state, but also in commercial contexts. Thus for instance, it is argued that the right to privacy is vital in order to guarantee the individual’s autonomy and his ability to choose freely and independently for himself how to conduct his life. In this sense Fried argues that privacy is a guarantee for personal freedom: if we know that all our actions are recorded, and that all that we say or do will be known to all, this is liable to influence the actions that we take. Transparency generally is not two-way, and gives the observing side the possibility to control the observed individual and to orient his behavior. The right to privacy was designed therefore to allow personal freedom and consolidation of an independent identity. In this sense the right to privacy constitutes an essential element in maintaining social relations and a basis for social solidarity. The assumption in this context is that an individual’s autonomy constitutes an important basis for his ability to establish authentic relations with the world.

---


234 See Fried, Privacy, supra note 229, p 210.

235 Jeremy Bentham coined the term “Panopticon” in the context of the “efficient” penitentiary. An efficient prison facility in his opinion will make control more efficient by centralizing the prisoners at the center of the facility, in a transparent structure exposed to the eyes of all the warders, at any given moment. This idea was subsequently expanded by Foucault who argued that the life of the individual in post-modern society is a life of transparency. The individual is exposed to all eyes and has nowhere to hide. For use of these terms in analysis of the risks of loss of privacy in the information age, see Oscar H. Gandy, Jr. The Panoptic Sort: A Political Economy of Personal Information (Boulder, 1993).

236 For this outlook oriented to the relation between privacy and autonomy of the individual, see: Nissenbaum, supra note 232; Julie E. Cohen, “Examined Lives” Informational Privacy and the Subject As Object”, 52 Stan. L. Rev. 1373 (2000).

237 For further discussion, see the lecture delivered by Dr. Moshe Cohen-Eliya at the Shefayim Conference, 26.12.01, evening session.

238 See Dr. Moshe Cohen-Eliya’s lecture, ibid.
3.2 Building identity and self-definition. Collection of information on the Web allows creation of a user profile disconnected from the person concerned by the information, and technically it can be used in various contexts without need for his collaboration. The ability to control the information is based on the individual’s power to define his identity towards himself, and towards others, and to prevent others from defining his image, personality and acts for him. As regards the ability to limit the use of personal information by commercial agencies, the right to privacy allows the individual not to become a commodity, to remove from his proximity commercial agencies in which he is not interested, and to choose to be in business or social contact with other agencies. The right to privacy in this context allows a person to participate in determining his place on the social ladder, and not to accept the commercial placement and the commercial possibilities of choice combined with it. In this sense, the right to privacy derives from an outlook of the individual’s autonomy and right to self-definition. 239

3.3 Exercise of other human rights – such as freedom of speech. The right to privacy is essential for the exercise of other civil rights, and primarily freedom of speech. When an individual knows that the state authorities are wiretapping or operating systems that can intercept any information and including also what he says, he will hesitate to speak absolutely freely. When a person knows that he is under surveillance, or that his words and deeds are recorded and stored, he is liable to avoid speaking freely. Sometimes the knowledge of the use of surveillance means, even if they are not actually used constantly, is sufficient to lead to self-censorship. This manifestation is known as the “chilling effect”. 240

There is a relation between privacy and anonymity. The possibility of transmitting messages anonymously on the Internet is one of the important tools in protection of privacy and empowering freedom of speech. This possibility, which includes the ability to transmit messages, to collect information or know-how without disclosing the surfer’s identity, gives the surfer great freedom of action that does not require disclosing of his true identity. This is a specific aspect of the right to privacy embodied in the expression “the right to be left alone”. Namely, the individual does

239 See Cohen-Eliya, Ibid.
240 Fried, Privacy, supra., note 229.
not wish specific actions to be attributed to him and therefore he chooses means of protection such as use of transmission of anonymous messages. Hacking into anonymous message transmission mechanisms in order to serve the public interest is liable to seriously prejudice freedom of speech on the Internet and to prejudice the privacy of the message sender. Naturally the question is to what extent anonymous expression should be allowed or even encouraged. On one hand, clearly the possibility of anonymous expression is likely to produce a richer public dialogue, including positions and information that would not reach the knowledge of the public if the speakers were required to reveal their identity. On the other hand, anonymous expression, that allows the speaker to deliver information or to express an opinion without liability for the results of his works, could cause damage. State secrets, for instance, might be exposed in this way, or unfounded statements might be published that could constitute defamation. Similarly, the possibility of anonymity could contribute to use of the Internet for terror acts.

The chilling effect of the lack of privacy on freedom of speech might be expressed also in another aspect of the right to freedom of speech – namely the right to seek, read and receive information. A person who knows that all his actions are recorded, is liable not to seek information and carry out searches for information in areas in which he is interested, for fear that this might cause him prejudice (for instance, search for information regarding drugs for a specific illness, sexual identity, or articles related to a political movement or a new social movement).

4. What are the limits of privacy in the information age?

Society’s right (through its proxy – the State) to protect public order establishes the moral justification for the existence of prevention and enforcement systems such as monitoring (wiretapping), search and seizure systems. This right, however clashes with the basic rights of individuals, including the right to privacy and the right to freedom of speech. The attempt to balance between security needs and the rights of the individual in the area of data collection on the Internet creates complex practical dilemmas. Should the State be given the right to eavesdrop on every conversation or piece of information passing through the Internet without control? Or should it be restricted to specific cases only? There are two practical methods that express
different formulas of checks and balances between the interests of state security and the rights of the individual.

The first way is to allow the State to intercept all information without filtering, and to analyze only the suspicious information. This possibility allows access a posteriori to information that initially does not seem dangerous. Take for instance the events of September 11, 2001; the messages that passed between the planners of the attack and those who perpetrated it did not arouse suspicion in real time. However, a posteriori, this information was extremely relevant in locating those responsible for the attack.

Nonetheless, interception of all the information traversing the Internet has many indirect effects on the rights of the surfers who express themselves through the Internet. Individuals who wish to transmit personal information not related to terror or harmful acts of one kind or another, will fear to do so since this information is intercepted and documented by the State, and they may fear that in due course the State will use the information against them. Take for instance lovers who both have separate families, who wish to express their feelings through messages on the Internet. The knowledge that their words are intercepted and stored by the State will cause cooling of the expression of their feelings and serious infringement of their privacy.

The second way of balancing between the interests of the State and the interests of the individual in the State, in the context of freedom of speech on the Internet, is to allow the State to eavesdrop on all information and to intercept only that which it suspects might be harmful to public order. This possibility guarantees that it will not be possible in the future to reconstruct information that was not intercepted. However, because of the fear that specific information might be relevant at a later stage, the definition of the degree of suspicion that allows interception will be broad and will include also expressions that do not constitute an immediate and clear threat to the public interest. There may, for instance, be a situation in which society will allow interception of messages of relatives of a terrorist only because of the suspicion that this channel might be used for transmission of harmful information. Monitoring of this channel will prejudice the freedom of speech and the privacy of the terrorist’s family even in situations where there is no indication of harmful speech by them.

The knowledge of a person’s right to data privacy imposes restrictions on the information users as regards collection, use and processing of the information. These
limitations on “freedom of the flow of information” might exact a heavy price. Information technologies make a tremendous contribution to efficiency and progress, in the field of commerce, for instance, in the reducing of costs and lowering of prices, in provision of new services, in saving human life in the case of health injury, and of course in fighting crime and terrorist organizations. Protection of privacy that imposes limitations on use of the information, is liable in many cases to prejudice other rights and interests. For instance, the right to receive information, the public’s right (and the State’s required obligation) to self-protection that also at times requires invasion of the privacy of one individual or another.

The scope of legal protection of the right to privacy depends on the balance between the right to privacy and other rights and interests that must be protected. In this context a distinction should be made between protection of privacy threatened by the State and protection of privacy against threats deriving from other individuals, such as commercial companies.

As regards the balance between the right to privacy and government needs, historically and culturally there are two main traditions: one wishes to limit the State’s surveillance power – from the Greek city-state (the polis), through the English Protestant movement and the accepted legal tradition, to the principles of the American Constitution and the proprietary rights therein. The second grants extensive powers to the government to monitor the individual, from Roman Sparta, through the medieval church, to the continental nation-state. Incidentally, it should be noted that Israel probably comes somewhere in between.

As regards protection of privacy in commercial contexts there is also a difference between the tradition manifest in American law and the continental tradition. In American law the protection of the right to privacy focuses on rights against invasion of privacy by the State, and is careful not to restrict the free activity of economic

---

241 The right to receive information implies a public interest and a private interest. The public interest is the public right to know (since information about the acts of individuals might be essential for all society). The individual’s interest is for shaping of his opinion and for this he requires information also about the private affairs of someone. See Zeev Segal, “Hazekhut Lepratiut Mul Hazekhut Ladaat” (The right to privacy versus the right to know) 9 Iyun Mispah (1983) 175, 178.

242 The formula of balance between the State security interest and the right to privacy in Israel will be discussed at length below in section (E). The standard legal regulation in Israel for search, seizure and secret monitoring erodes protection of the individual’s right to privacy. Israeli law was designed to guarantee that prejudice to a person’s privacy for protection of security means, would be allowed only if public interest prevails over the right to privacy.
agencies working in the free market and using private information as an economic resource to all intents and purposes. The European approach, on the other hand, emphasizes collection and use of private information by commercial organizations.

Balance is required also in the context of freedom of speech. The scope of freedom of speech is directly affected by the degree of protection given it. Freedom of speech in its absolute sense is the freedom to express opinions in any way without any fear of prejudice to any interest of the speaker. The more extensive the freedom of speech, the more individuals will tend to speak more freely. The information age in general and the Internet in particular bring the discussion of freedom of speech to a new level.

The Internet and the information flowing in it constitute “a free market of ideas”, providing a platform to anyone who so wishes and allowing surfers to share their opinion without any geographic restriction whatsoever. The capacity to transmit messages to millions by the press of the button and at low cost makes the Internet the most democratic communications means created until now. These advantages, which allow free speech and free flow of information on one hand, and society’s wish for control on the information passing through the Internet on the other, establish a real legislative obstacle for the State’s activities. Freedom of speech constitutes the secret of the Internet’s charm. This distinctive feature is prejudiced when the State operates surveillance means on the contents and messages passing through the Internet with the aim of protecting the public interest in general and public order in particular. Any attempt by the State to control events on the Internet, and to collect or intercept speech on the Internet by eavesdropping, listening and surveillance systems, is liable to prejudice the individual’s right to freedom of speech and privacy.

In the discussion below we will examine how these approaches are expressed in the existing legal regulations as regards surveillance and search actions. Subsequently we will examine whether the regulations are suited to prevention and enforcement actions on the Internet.

D. Legal Limitations on Acts of Prevention and Enforcement in the Information Age

1. The Legal Framework

The means of prevention and enforcement operated by the government authorities are demarcated, at least on the face of it, by regulations and principles of public law. Firstly, the state authorities are subject to the constitutional law and basic rights recognized as a normative framework, wherein all the activities will be subject to balances vis-à-vis basic human rights. Secondly, the authorities are subject to the principles of administrative law, and these delineate a general framework of action in pursuance of the principle of legality, since the authority only has what the law gives it. The authority cannot operate means of prevention and enforcement without legal empowerment for this action. Further, the existence of the power is not sufficient. The authority must act reasonably and fairly, and at the same time must also take into account human rights considerations as noted above. Thirdly, the authority’s action is subject to the constant possibility of judicial control. Moreover, judicial control is possible over all the stages, both before implementation of means of prevention and enforcement (when applying for required warrants) and afterwards, whether by direct or indirect attack.

In this section we will review the relevant laws at the international level, in the USA, in the European Union and in other countries. In reviewing the laws we will highlight in particular new legislation that came into force, although it did not necessarily originate, after the events of September 11. Special emphasis will be placed on the new American law, the USA Patriot Act, and on a new British law passed in late December 2001: the Anti-Terrorism, Crime and Security Act. After reviewing the laws, we will deal separately with commercial agencies and obligations that were imposed on them as regards collection, storing and delivering of information to the enforcement agencies. In this context, an extensive framework for discussion can be found in the new Convention on CyberCrime of November 2001, which considerably expands the category of “service providers”.
2. The International Context

2.1 Protection of the Right to Privacy

Modern treatment of the right to privacy at the international level is found in the Universal Declaration of Human Rights of 1948. A large number of general international treaties expressly recognize the right to privacy, including the International Covenant on Civil and Political Rights (ICCPR) and UN treaties. At the regional level, there are conventions that have made the right to privacy a legally enforceable right: for instance, the European Convention of Human Rights and Fundamental Freedoms of 1950. In pursuance of this convention the European Human Rights Commission, the European Human Rights Court and the Charter of Fundamental Rights of the European Community, protecting privacy and personal information, were established.

The recognition of the right to privacy in international law provides a foundation for the right to privacy as a basic human right in any situation that arises. Moreover, most Western countries recognize the right at the level of national law as a constitutional right, namely at the normative level also for regular constitutional matters. Further,

---

245 **Universal Bill of Human Rights** (1948) section 12: 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. [http://www.hrweb.org/legal/udhr.html](http://www.hrweb.org/legal/udhr.html) (last visit: 23.12.01).

246 **International Covenant on Civil and Political Rights (1966)**, Article 17:

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
2. Everybody has the right to the protection of the law against such interference or attacks.

[http://www.hrweb.org/legal/cpr.html](http://www.hrweb.org/legal/cpr.html) last visit: (23.12.01)

247 See **European Convention of Human Rights & Fundamental Freedoms (1950)**, Art. 8:

1. Everybody has the right to respect for his private and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the rights and freedoms of others.” There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the rights and freedoms of others.”

more recent constitutions deal specifically with the right to privacy and the right to control personal information. Forty out of the fifty countries reviewed in the year 2000 report of the Organization for Protection of Privacy, (including Israel) demonstrated awareness and clear rights as regards access to public documentation.\textsuperscript{249} The protection at the international level and the recognition of the right to privacy in the national law of many countries around the world indicate the great importance of the right to privacy, and are liable to have a direct influence on the checks and balances required in every situation in which the right might be prejudiced, particularly in the political climate created after the events of September 11 and in light of new technologies allowing unprecedented invasion of privacy.

### 2.2 International Regulation for Protection of Personal Data

The right to privacy also applies in specific cases concerning the right of the individual to prevent collection and processing of personal data concerning him. International protection of electronic data concerning the individual exists in a convention of 1990: \textit{Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data}.\textsuperscript{250} This convention discusses personal data files and processing of data in the public sector and the private sector. It stipulates that obtaining, processing and storage of data will be conducted in accordance with the objects for which it was collected. The data must be proper, relevant and must not deviate from the objects for which it was collected and stored. The holder of the data must guarantee the exactness of the data, including the possibility of periodic correction and updating. However at the same time he must implement appropriate means of protection to safeguard the data from unauthorized access or modification. According to the convention, the means of protection of a person’s privacy must be verified. Accordingly persons whose details are included in the data, must receive access to the information in such a way as to guarantee the possibility of determining the existence of the data file, its object and the identity of the agency controlling the

\textsuperscript{249} This is a survey conducted by the Center for Electronic Privacy in Washington and the International Center for Privacy in London. The report reviews the status of the right to privacy in some fifty countries, and examines in them areas of privacy, including data protection, wiretapping, data banks, identification systems and freedom of information. At: \url{www.privacyinternational.org/survey/phr2000/html} (last visit: 23.12.01).

data; the possibility of receiving confirmation that the personal data is indeed stored; the possibility of obtaining correction or deletion contrary to local law. Nonetheless, the convention recognizes exceptions that will be anchored in national legislation in countries, for purposes of protecting state security, public security and the financial affairs of the State, and also for purposes of enforcing criminal law or when the step is necessary in order to defend rights of others.\(^\text{251}\)

This regulation, even though it is at the level of guidelines only and does not constitute normative law, is found in the UN guidelines: United Nations Guidelines Concerning Computerized Personal Data Files.\(^\text{252}\) This document establishes an orientation only. Implementation of the regulation in relation to automated personal data was left to each country’s discretion. The guidelines define a series of principles in relation to a minimum standard of privacy at the national level:

- **Principle of lawfulness and fairness** - Information about persons should not be collected or processed in unfair or unlawful ways.
- **Accuracy** - Persons responsible for keeping the data have an obligation to conduct regular checks on the accuracy and relevance of the data recorded.
- **Purpose-specification** – The purpose for which the data is collected must be specified, legitimate and known, so that it will be possible to limit the storage to the area, time and capacity of use.
- **Access** – Anyone who offers proof of identity has the right to know whether information concerning him is being collected.
- **Non-discrimination** - Subject to cases of exceptions, data likely to give rise to discrimination, including information on racial or ethnic origin, color, sex life, political opinions, religious, philosophical and other beliefs as well as membership of an association or trade union, should not be compiled.
- **Power to make exceptions** - Departures may be authorized only if they are necessary to protect national security, public order, public health or morality, as well as the rights of others provided that such departures are expressly specified in a law and their limits are expressly stated. As regards the


prohibition of discrimination and data related thereto, additional safeguards are required within the limits prescribed by the International Bill of Human Rights.

- **Security** - Appropriate measures should be taken to protect data files against accidental loss or destruction and intentional tampering.

- **Supervision and Sanctions** - The law of every country shall designate the authority that is to be responsible for supervising observance of the principles set forth above. In the event of violation, criminal or other penalties should be envisaged together with the appropriate individual remedies.

- **Transborder data flows** - When the legislation of two or more countries concerned by a transborder data flow offers comparable safeguards for the protection of privacy, information should be able to circulate as freely as inside each of the territories concerned.

- **Application** – The principles should also be extended to data that is not stored by computerized means. The principles also propose implementation of the principles in relation to data files in the possession of government agencies, subject to appropriate adjustments.253

Another international regulation, although its normative importance is far lesser, exists in the form of the OECD guidelines on electronic data: **OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data, Recommendation of the Council**.254 These guidelines set down the basic principles regarding collection, use and disclosure of personal data and information. The guidelines call for a restriction to be imposed on collection of personal data in local law, transparency as regards the object of collection of the information and according to the use, possible disclosure only by consent, development of protections anchored in law, adopting of a policy of openness as regards personal data, and safeguarding the right of the individual to receive confirmation that data concerning him was collected, to study the data, to verify that it is correct and to protest data that is erroneous.255 Other international provisions can be found in the European Union.


3. The European Union

The European Union exists by virtue of the treaties that created it (Treaty of Rome, the Single European Act and the Treaty of Maastricht). In pursuance of these treaties certain areas were placed from the start in the Community’s sole jurisdiction, a few areas were made subordinate to a kind of “parallel authority” and others were left in the exclusive authority of the individual countries.256 Therefore there exist qualifications in the different legislative items of the European Union,257 concerning fields that were left outside the Union’s jurisdiction, such as issues of security and general state interests (unlike economic interests) and a possibility of local legislation that will allow exceptions to the provisions in these cases. Another aspect of division of the powers cited above can be found in the various legislative items relating mainly to the private sector and not to the enforcement authorities in the different countries. Such treatment can be found mainly in the context of imposing obligations on a private entity (such as service providers) to act in accordance with the demands of the enforcement authorities.

In this section we will review establishing of a framework of action in the European Union in the area of protection of personal data and other directives that expanded this line of action. We will then discuss the legal framework created after September 11, with most of the discussion being devoted to the convention on cyber-crime opened for signatures of the countries, and the new British law, designed to handle the need to give appropriate powers to the enforcement agencies for overcoming terror as against the need to safeguard human rights in the country.

257 The Community legislation is made up of four types of legislation: The treaty (convention) is the supreme legislative item, and therefore it can be compared to a law in a federal state, but it does not have direct application within the countries; regulations, which are considered the legislative item closest to normative legislation in a sovereign state, and which constitute the only legislative item in the Union that is directly applicable; directives are an “original” Community creation in that they are the legislation that determines binding objectives, but leaves the member countries to determine the ways of implementing the objective. The use of regulations is more accepted in those fields where the EU has clear jurisdiction and as a tool for bringing the domestic law of the member countries into line; decisions which are at the lowest level on the normative scale and resemble an individual order. See Lev, Ibid. at 43-45.
3.1 The EU Directive on Data Protection

The EU Directive on Data Protection of 1995\textsuperscript{258} obliges the member countries to promulgate laws that will apply to the private sector on the right to privacy in relation to collection, processing, storage and transmission of personal data. This Directive in fact allowed free movement of electronic data between countries of the EU, while guaranteeing that individuals would enjoy a high level of protection from abuse of the data.\textsuperscript{259} The main points of the Directive:

Personal data is defined in the Directive as any information relating to an identified person or a person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

The Directive defines several exceptions to application of the regulation. Article 3(2) stipulates situations in which application to the entire data processing activity is qualified:

- In the course of an activity which falls outside the scope of Community law (in pursuance of the founding Treaty) and in any case of processing operations concerning public security, defense, State security (including the economic well-being of the State) and the activities of the State in areas of criminal law. In the framework of the treaties establishing the European Union, it was agreed that these laws would remain in the jurisdiction of the member countries and this is the reason for the exception.
- Processing of data by a natural person in the course of a purely personal or household activity.
- It should be remembered that while the domestic legislation in each country must be promulgated in the spirit of the Directive, Article 5 expressly stipulates that the countries may determine more precisely the conditions under which the processing of personal data is lawful.


\textsuperscript{259} Bar-Sadeh, supra note 251, at 187.
In pursuance of the Directive, every business must meet several conditions. Inter alia, it must be guaranteed that personal data collected from customers will be processed in a legitimate and fair way, for specific, explicit and legitimate purposes, and that the data will be kept updated and properly stored. In addition the business must notify the customers of the person responsible for the data, the right to access the data and the right to correct it. The Directive emphasizes that once collected, the material will be processed only with the customer’s clear consent thereto. Violation of the obligations acquires for the data subject the right to compensation, and the remedies will be accorded in pursuance of the laws of the Member state. The countries are also required to establish an independent supervisory body with a variety of powers, including, investigation, monitoring and blocking.

In relation to countries outside the EU, there is a prohibition on transfer of personal data to countries not complying with the European data protection standard. The USA and the European Union reached an agreement called the “safe harbor framework” whereby American companies will be considered to meet the standard, while being granted the possibility of independent, non-governmental regulation, in pursuance of seven basic principles: notice, choice, limitation of onward transfer, security, data integrity, access and enforcement.260

As regards other countries, on 4.12.01 the committee of member states approved a proposal of the Commission for standard contractual articles to be adopted by data-processing organizations in countries outside the EU. This means was designed to prevent refusal of onward data transfer because of noncompliance with the treaty requirements.261

3.2 Implementation of the Directive by the Member States

Although the Directive dates from 1995, the relevant legislation in many countries came into force only in early 2000. Furthermore, proceedings were instituted against five countries in the European court because of delay in adopting appropriate legislation in accordance with the schedule determined in the Directive (Luxembourg,

---

260 For the 13.02.2002 report of the EU committee that recently examined implementation of the agreement between the USA and the EU regarding protection of personal data, see http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf (last visit: 18.2.02).

Ireland, Germany, France and Denmark). Of those countries only in Denmark has the required law been promulgated in the meantime, coming into force in July 2000.\textsuperscript{262}

The 1995 Directive for protection of personal data created in the European Union a comprehensive working framework, in which the other directives and decisions were adopted that expand the scope of application of the principles. Other comprehensive provisions were adopted in relation to the telecommunications market, dealing in the main part with various obligations imposed on ISP’s. Accordingly they will be discussed separately in the section on data collection by commercial organizations below.

3.3. Legal Developments after September 11

Convention on Cybercrime 2001

After September 11 another convention was signed that is liable to affect the enforcement powers and the relations between the State and the service providers. This is the international Convention on Cybercrime, which originated with the European Union.\textsuperscript{263} The convention was opened for the signature of the European countries and other countries that participated in its formulation (Israel was not one of them). Since November until the date of writing this paper (December 2001) 31 countries have signed the convention, including the USA, Canada and Japan. The convention will come into force only after five countries ratify it (integrate the convention into their national law) and of these at least three must be members of the Council of Europe.\textsuperscript{264}

The explanatory notes\textsuperscript{265} clarify that the aim of the convention is to realize three main objectives: (1) harmonization of national criminal law in fields of cybercrime; (2) granting national procedural powers required for investigation and prosecution for cybercrime and other offenses committed using computer systems; (3) establishing an...
efficient framework for international cooperation. In pursuance of these objectives, the covenant is made up of four chapters: terms, measures to be taken at the national level as regards substantive law and as regards procedural law, international cooperation and articles of reservations and application. The convention defines nine offenses as substantive law: illegal access, illegal interception, system interference, misuse of devices, computer-related forgery, computer-related fraud, child pornography, and offenses related to infringements of copyright and related rights. Areas covered by procedural law apply not only to the basic offenses indicated above, but also to any offense carried out using computer systems or where the proofs of the offense are by electronic means. The convention defines a series of powers granted to the enforcement authorities:

- Expedited preservation of stored data – Article 16.
- Expedited preservation and partial disclosure of traffic data – Article 17.
- Production order – Article 18.
- Search and seizure of computer data – Article 19.
- Real-time collection of traffic data – Article 20.
- Interception of content data – Article 21.

All the powers given to the authorities are subject to Articles 14-15 of the covenant, whereby the powers are delimited by specific conditions and legally defined.

The third chapter of the covenant defines additional provisions regarding traditional computer crimes and provisions for international cooperation including principles of extradition. The provisions deal with international assistance in two types of cases: When there is a legal base in the form of treaties, reciprocal legislation etc., then the existing agreement will be expanded also to situations cited in the covenant, and if there is no prior legal base, the provisions stipulated in this chapter will apply. The chapter also contains a special provision on trans-border access to stored computer data that does not require mutual assistance (with consent or where publicly available) and allows the creation of a network designed to guarantee rapid assistance between signatory countries of the covenant.
Article 22 deals with jurisdiction and sets down a series of criteria in pursuance of which parties are bound to establish a jurisdiction over criminal offenses stipulated in the covenant. This is based on well-known territorial and national principles. The Article also allows the creation of additional jurisdictional bases in the framework of national law. In cases where a jurisdiction is established for more than one country, for instance in trans-border virus attacks on the Internet, the relevant countries shall consult with each other in order to determine in which country the trial will be held. Another important article is Article 42, which deals with reservations and allows several reservations (this is a closed list) in light of the nature and character of the Covenant.

3.4 The New British Anti-Terrorism Act
A new and comprehensive law was recently promulgated by the British Parliament: **Anti-terrorism, Crime and Security Act 2001.** The object of the law was to amend the anti-terrorism law passed in the year 2000, and to lay down additional provisions on terror and security. Inter alia, and in our context, the law extends the prevention and enforcement powers of the government authorities, allows storage of traffic data for a long period and lays down provisions for disclosure of information to the authorities. The law also deals with a series of fields including handling of property and money of terrorist organizations, immigration, xenophobic offenses, weapons of mass destruction, safety of poisons and nuclear industry, security in the field of aviation, bribery and extortion, etc.

3.5 Data Collection by ISP’s
**CyberCrime Treaty**
The Convention on Cybercrime discussed above deals extensively with imposing obligations on service providers, in the overall framework of procedural steps and


107
powers granted to the enforcement authorities. Firstly, it should be noted that this covenant gives an extremely broad definition to the term “service provider.” The term is designed to include a broad category of natural and legal persons serving in a specific role in communications or processing of data in computer systems. In pursuance of this definition, clearly both public and private entities that provide users with the ability to communicate with others are included in the definition. Therefore, the question of whether the users create a closed group or whether the service is offered to the public, or whether the service is free of charge or against payment, is irrelevant. The closed group to which the service is provided can be employees in a private company to whom the service is proposed by way of the company server. The definition also includes entities that store or process in another way information for the entities cited above or for the users. For instance the definition includes “hosting” and “caching” services, and Internet connection services. At the same time, a contents provider only is not meant to be included in the definition of “service provider, and provided that it does not also offer connection or data processing services. 

In the framework of the procedural powers established by the convention, obligations are imposed on the service providers. Section 18 of the Convention calls for legislation by which the authorities will be able to oblige the service provider to transmit customer information, through which it will be possible to establish the type of communication, the subscriber’s identity and geographic location. In pursuance of sections 20-21, the service providers will also be obligated to furnish information on contents and communication in real time on the communications on their servers. It should also be noted that despite the existence of sections requiring clear limitations and anchoring in legislation, the Convention makes it possible to demand that the service provider maintains confidentiality also in the framework of the cooperation with the authorities, and one may wonder what effect this obligation of confidentially on one hand, and the ability to oblige the providers to furnish information on the other, will have on the commercial (and legal) relations between the service provider and the consumers.

Another important item of British legislation is the **Regulation of Investigatory Powers Act 2000**. Practically, the legislation obliges service providers to disclose encryption keys or location of the keys, but its object is to guarantee a fitting balance between the ability of the enforcement authorities to interfere in electronic transmissions and the establishing of essential protection of the rights of the individual and the business interests that must be protected at the time of such activity by the authorities. The regulations deal with four different actions: interception of transmissions, close surveillance, human data sources and disclosure of encrypted information. It will be possible to carry out the actions only after receipt of a corresponding order, which must be based on proof of one of the following causes: the action is for the sake of national security, to prevent a serious crime or to guarantee British economic interests.

Subject to the legal provisions, the service provider will now be subject to a legal obligation to grant access to transmissions, and to disclose any protected information, namely any encrypted information, whether in transmissions still in progress, or in information stored with the service provider. It should be noted that there is a position that the legality of the law is doubtful in light of the European Human Rights Convention, which was assimilated, in British law in the **Human Rights Act 1998**.  

### The Telecommunications Sector

The field of telecommunications has been the subject of extensive legislation in the European Union, as part of the orientation to guarantee free competition in this market. In the framework of the regulation the field of privacy was also dealt with in the **EU Directive on Personal Data and Privacy in the Telecommunication Sector**. The directive imposes a broad range of obligations on service providers to guarantee the privacy of the users of communications means, including activities related to the Internet. The rules relate to fields, which, prior to these directives, in fact fell between the cracks in the general framework of data protection laws. They apply to processing of personal data in the context of telecommunications services.

---

268 Ibid.at 60.

available to the public in the EU, and particularly digital services (Integrated Services Digital Network-ISDN) and the field of mobile telephones.

The Directive imposes restrictions on access to the information. The Caller ID technology must incorporate the possibility of blocking the transmitted number. Information collected in delivery of the communication must be “cleansed” on conclusion of the call. Subscribers are entitled to receive non-itemized bills. The provider must allow the subscriber to block automated calls arriving from third parties. Subscriber directories must be limited to essential details only. Use for marketing purposes by recorded advertising and sending of faxes must be limited to subscribers who have given their consent thereto.

As a continuation of this directive, the Commission proposed in July 2000 a directive on data processing and protection of privacy in the electronic communications sector. The proposal was submitted as part of the overall package, with the aim of reinforcing the electronic communications competition in the European market. The proposal is that the directive would replace the existing directive of 1997, by extending the existing protection for communications of the individual to a broader technological and legal category of “electronic communications”. The proposal replaces existing definitions of telecommunication services and networks by a new definition of electronic communication services and networks. In addition, the proposal adds new definitions and protections for calls, connections, traffic data and location data, with the aim of reinforcing the consumer’s right to privacy and giving a possibility of control in processing of different types of data.

These proposed provisions will guarantee, for instance, the protection of all the data related to Internet transmissions, will ban unsolicited marketing by e-mail (Spam) without prior consent by the “opt-in” method, and will give mobile telephone users protection from immediate place location and from wiretapping. The proposed directive also allows the subscribers to the servers and the providers to choose whether they wish to be entered in public directories. However, it should be noted that

---

this proposed directive also gives the countries a possibility of limiting its provisions with security and enforcement need restrictions. This proposal was discussed in the European parliament, which has already transmitted a few amendments, in order to allow Spam and to restrict saving of the information of the service providers to law enforcement purposes. In pursuance of the amendment, any surveillance and monitoring must be essential, appropriate, proportional and limited in time. The means must be anchored in jurisprudence and approved on an individual basis and by a relevant authority subject to the commitment to the European Human Rights Convention and the ruling of the Human Rights Court, so that extensive or general electronic surveillance is not possible.

Personal Data and Electronic Signatures

EU Directive 1999/93/EC on Electronic Signatures: This directive extends the provisions of the directive on personal data and imposes a supervisory and data storage obligation on certification service providers. These entities may collect personal data only directly from the data subject or after receipt of his explicit consent, and only in relation to what is required and obligatory for purposes of issuing the certification. The data must not be collected for other purposes (Article 8).

4. The USA

4.1 General Background

The right to privacy is protected in the USA by the Fourth Amendment to the Constitution:

“The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and

272 For amendment of the directive in the framework of the European Parliament committees, see: http://www.privacyinternational.org/issues/cybercrime/index.html#coe (24.12.01).
particularly describing the place to be searched, and the persons or things to be seized.\footnote{274}{U.S. Const. Amend. IV.}

The Fourth Amendment restricts the government powers to invade the privacy of the country’s citizens and obliges the government not to infringe these rights without legal cause. The Fourth Amendment sets a standard of “probable cause”,\footnote{275}{See United States v. Cavanagh, 807 F.2d 787 (9th Cir. 1987).} when the government wishes to intercept communications or receive a search warrant, since carrying out of actions of this kind may infringe the right to privacy of the person under surveillance and of others. The cause must be specified in the oath. There is also a system of checks and balances in the various laws and case law.

In October 2001 the USA PATRIOT Act was promulgated. This Act reinforces and extends the surveillance powers of the US domestic law enforcement authorities and of the international intelligence agencies. It is argued by some that this Act modifies the system of checks and balances that was shaped in the 1970, following the uncontrolled use made of surveillance powers by the different agencies (over 10,000 citizens were placed under permanent surveillance, including Martin Luther King). For instance, in pursuance of the new law, for the court to oblige a service provider to deliver mail logs and addresses of a specific person, the standard required is only that the government will present facts whereby it is reasonable to believe that the records are relevant to an investigation in progress. The question is whether this standard corresponds to the “probable cause” condition in the Fourth Amendment. On the other hand there are those who argue that a distinction must be made between collection of “content data” concerning a specific person and collection of “numerical information” (e.g. numbers that he dialed, or e-mail addresses with which he corresponded), for which the collection standard can be lower.

The new Act introduces modifications in some fifteen existing laws. Many of these amendments infringe the right to privacy in the electronic communications between citizens. The government may now be entitled to monitor innocent surfers if they keyed in a concept that “arouses suspicion” in an Internet search engine – all that the government has to do is to swear before a court that the act might lead to information
relevant to an investigation in progress. The person whose computer is monitored does not have to be the subject of an investigation or suspected of any crime.

4.2 Legal control of invasion of privacy by the enforcement agencies.
American law recognizes four surveillance means: interception of broadcasts including wiretapping (interception orders), search and seize orders of actual objects (search warrants), orders for locating to whom or from where a call was made (pen/trap orders) and subpoena and court orders (for obtaining of information). The various warrants and orders require a different level of certainty and legal intervention in direct relation to the invasion of rights such as privacy and freedom of speech.

4.2.1 Secret monitoring and interception
a. Outside US borders
The intelligence agencies are not restricted in employment of surveillance means outside the USA. There is no legislation in the matter, apart from a directive of President Reagan, which is valid to this day.276 The directive establishes that if a United States person is the subject of secret monitoring,277 authorization must be received from the Attorney General, who has the power to decide whether there is probable cause that the target is a foreign agent.

b. Within the USA.
Two laws regulate surveillance within the USA. One is the Federal Wiretap Act (1968),278 which allows operation of surveillance and secret monitoring means, through a court order, after it found, on the basis of the State oath, that there is probable cause that a crime was committed, is being committed or will be committed. The law contains a closed list of crimes for which an order can be given in the

277 “United States person” means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an associated which is a foreign power, as defined in 50 U.S.C. §1801(a)(1), (2), or (3). See 50 U.S.C. §1801(i).
278 The Omnibus Crime Control and Safe Streets Act of 1968 commonly known as the “wiretap law.”
framework of this law.\textsuperscript{279} In the new law,\textsuperscript{280} terror acts and offenses in pursuance of the Computer Fraud and Abuse Act were added to the list.\textsuperscript{281}

The Foreign Intelligence Surveillance Act of 1978 (FISA)\textsuperscript{282} allows issuing of wiretapping orders, by a special court, for agents of a foreign power.\textsuperscript{283} Here too probable cause must be shown. However, for issuing of an order for someone who is a US person, it must be shown that the information is essential for national security, whereas as regards a person who is not a US person, it must be shown that the information is related to national security. The definitions of an agent of a foreign power should be noted: according to this definition the membership of a US citizen in a terror organization does not correspond to the definition of an “agent of a foreign power”. For this the citizen must work to advance the terrorist objects. The distinction lies in the protection that the First Amendment gives to American citizens whereby membership and activity in a terror organization may be for advancement of a specific idea, and the citizen cannot be systematically prevented from expressing his opinion. In emergencies (to protect life and limb) it is possible to implement surveillance means in pursuance of both laws even without a court order.

\textsuperscript{279} 18 U.S.C. §2516(1).
\textsuperscript{280} USA PATRIOT Act §§ 201-202.
\textsuperscript{281} Computer Fraud and Abuse Act (CFAA), 18 USC §1030.
\textsuperscript{283} See: United States Signals Intelligence Directive, 27 July 1993. The term ‘Agent of a foreign power’ is defined as follows:

a. Any person, other than a U.S. person, who:
(1) Acts in the United States as an officer or employee of a foreign power, or as a member of a group engaged in international terrorism or activities in preparation therefor;
(2) Acts for, or on behalf of, a foreign power that engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person’s presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities;

b. Any person, including a U.S. person, who:
(1) Knowingly engages in clandestine intelligence gathering activities for, or on behalf of, a foreign power, which activities involve, or may involve a violation of the criminal statutes of the United States; or
(2) Pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for, or on behalf of, such foreign power, which activities involve or are about to involve, a violation of the criminal statutes of the United States; or
(3) Knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for, or on behalf of, a foreign power; or
(4) Knowingly aids or abets any person in the conduct of activities described in paragraphs 9.1.b.(1) through (3) or knowingly conspires with any person to engage in such activities.
4.2.2 Pen/Trap Orders

The purpose of the orders is to find the location of outgoing or incoming calls. The courts approve the orders as long as they can provide relevant information for a criminal offense. The court’s discretion is mainly technical as regards the manner of filing the application. Section 216 of the new Act extends the authorization for tracing of calls from line communications and adds electronic communications. Section 214 of the new Act also extended the possibilities of issuing the warrant in the counterintelligence framework (FISA) to cases of terror, but forbids opening of an investigation against a citizen only on account of information protected by the First Amendment (Freedom of Speech). The FBI’s Carnivore carries out similar activity on the Internet. The system is located at large data nodes and traces the source and the target of the messages transmitted over the Internet. The problem created is that the system actually scans a very large quantity of data, in order to find a specific piece of information for which the trace has been authorized only, and in addition, it is impossible to separate between the content and the data concerning the target, since they are transmitted together. Since the FBI does not specify the method of operation of the existing system, it is feared that the system collects information on contents and not only on the sender and recipient of the message.

4.2.3 Search and Seizure Orders

Search warrants are taken out with the authorization of a judge when there is probable cause that a crime was committed. At the time of or after execution of the search, the owner of the premises must be notified that a search was carried out. However the new Act extended the power to carrying out of secret searches in which the owner of the premises does not know that a search was carried out in his property/belongings. Search warrants serve for seizing of contents data that was received and stored by electronic means, including e-mail not yet read. The new Act allows interception of line communication stored data including voice mailbox, by search warrant. Under FISA, it is possible to carry out searches, without judicial control, with the

---

284 “Pen registers” are devices used to record telephone numbers that are dialed from a telephone, “trace devices” are used to determine where a telephone call originated.
286 USA PATRIOT Act, §214.
287 http://www.eff.org/Privacy/Surveillance/Carnivore/20000728_eff_house_carnivore.html
288 18 USC §2703 (a) and (b).
289 USA PATRIOT Act, §209.
authorization of the Attorney General. An investigation, in the framework of this law, and also a search against a US citizen, will not be carried out on account of speech protected by the First Constitutional Amendment.

4.2.4 Receipt of Information Collected by Access Providers

The enforcement agencies may order and receive information for purposes of carrying out investigations. Ordering of the information is not subject to legal control. The new Act empowers the enforcement agencies to order and receive from access and communications providers more extensive information than in the past, including time and duration of the call/Internet surfing, IP address, method of payments and details of the person making the payment. The authorities can order commercial records such as data on transactions carried out by e-commerce and any non-contents information related to access provision subscribers.

Section 217 of the new law allows study of information seized in computer trespasser communications. The rationale is that anyone hacking into a computer cannot expect privacy of his data. The new Act allows the service provider to deliver non-contents data, without a warrant, voluntarily, to protect life and limb.

The Communications Assistance for Law Enforcement Act (CALEA) demands that the communications companies adapt their systems to operation of control means by the enforcement agencies.

5. Other Countries

5.1 Canada

Personal Information Protection & Electronic Documents Act 2000

The object of the Canadian law was to regulate personal, financial and medical data privacy, and to create reliable and uniform regulation for e-commerce and electronic

---

290 50 USC §1822.
291 USA PATRIOT Act, §§210, 211.
292 18 USC §2703 (c).
293 USA PATRIOT Act §217.
294 USA PATRIOT Act, §212.
documents. The law was designed to give the individual personal data protection rights. The law defines the methods by which organizations can collect and use personal data, and the rights of the individual to access and modify the data. The law requires that businesses disclose the object of collection of the data and receive consent before collecting it. It should be noted that the law does not except from application non-Canadian companies, so that application of the law can include entities that are not Canadian but collect data in Canada or on Canadian citizens. The law also indicates that its object is to adapt the legal situation in Canada to the requirements defined in the European directive discussed above. Subordination to the law is being effected gradually so that certain commercial entities are already subject to it; from 2002 medical entities will also have to meet its requirements, and from 2004 all organizations will be subject to the law.

The legal situation after September 11

In Canada there is currently a process underway, influenced to a great extent by the events of September eleventh, that will lead to amendment of the local criminal law - **C-6 Anti-Terrorism Bill**. This amendment introduces into the criminal code several new sections, designed to fight terror. The new offenses that were added extend the existing law in relation to a group of situations considered situations of terrorist activity, for instance an offense against an international personage, or UN personnel, offenses that involve use of explosives or other lethal devices and offenses relating to funding of terror acts.

5.2 Australia

**Privacy Amendment (Private Sector) Act 2000**

In Australia the Privacy Protection Law was amended recently. The law relates, inter alia, to management of company information systems and seeks to protect personal and sensitive electronic data. The law, which came into force in December 2000, sets in NPP4 two basic requirements:

---

296 The Canadian parliament passed the amendment on 28.11.01, and the amendment was submitted for approval by the Senate, after which the law returns to Parliament for implementation. [http://www.canadianliberty.bc.ca/](http://www.canadianliberty.bc.ca/) (24.12.01).

1. Protection of personal data from misuse and unauthorized access, modifications or disclosure.
2. Destruction or permanent de-identification of unnecessary information.

According to the principle of NPP4 “reasonable steps” must be taken to safeguard physical security of the data, security of the computer systems and networks, and existence of safe communications; appropriate training of the staff of workers is also required.

**The Legal Situation after September 11**

After the events of September 11, several cyber-crime laws were legislated in Australia, including cyber-crimes carrying a ten-year prison sentence. In fact, the law deals with “standard” computer offenses and offenses by means of computer, such as unauthorized use, and allows investigative capacities also for “pure” criminal cases such as murder and fraud. The law included seven new “high-tech” offenses that covered hackers, prevention of service attacks, vandalism at sites, dissemination of viruses and use of computers in offenses such as harassment, fraud and sabotage. 298

**E. The Legal Framework: Israel**

1. **Introduction**

The right to privacy is a constitutional basic right anchored in a Basic Law: Human Dignity and Liberty. 299 The constitutional status guarantees that any violation thereof must be done in accordance with a term of the restriction clause, namely the violation must be committed legally, or by virtue of the law, it must correspond to the values of the State of Israel as a Jewish and democratic state, it must have an appropriate object, and be only to the required extent. 300 In light of the importance of the right to privacy, the Knesset saw fit to anchor protection thereof in law even before its constitutional anchoring. In 1981 the Privacy Protection Law 5741-1981 was promulgated. 301 In pursuance of this law, intentional violation of the right to privacy is a criminal

---

298 [http://australianit.news.com.au/articles/0,7204,2944524%5E15306%5E%5Enbv%5E,00.html](http://australianit.news.com.au/articles/0,7204,2944524%5E15306%5E%5Enbv%5E,00.html) (last visit: 24.12.01).
299 Section 7 of the Basic Law: Human Dignity and Liberty.
300 Section 8 of the Basic Law: Human Dignity and Liberty.
301 Privacy Protection Law, 1981.
offense. The rationale for this serious ruling, that sets before society an extremely high behavioral norm, is the viewpoint that those who violate a person’s privacy will not be deterred by a financial penalty only. If the violation of privacy was committed in circumstances in which a legal, moral, social or professional obligation to do so is imposed on the person responsible, he will be protected from civil or criminal action. The terms of moral and social obligation are regulator terms, which contain a danger of expansion of the scope of permitted infringement of privacy.

By means of the Privacy Protection Law the Knesset sought to provide a legal solution for worsening of infringement of privacy, in wake of the spread of mass means of communication, development of technological devices allowing wiretapping, remote tracking and detection, and growth of their dissemination, and in light of the expansion of collection and centralization of information in the hands of public and private entities. However, the Privacy Protection Law does not discuss the subject of data collection in computer centers, assuming that this subject would be regulated in separate legislation. Automated data collection is also not listed in Section 2 of the Law as possible violation of privacy. Notwithstanding, this list is an open list, which can be completed by the courts, out of an awareness that technological development is liable to create in the future methods of violation, which could not have been foreseen at the time of promulgation of the law in 1981. Only in Chapter 2 of the Privacy Protection Law, which deals with protection of databank privacy, did the Knesset deal with a limited aspect of infringement by technological development of the right to privacy, knowing that absence of effective protection of the tremendous personal data stored in computers might lead to serious injury of the individual. In this section we will review the legal regulations that allow invasion of privacy in Israel in the field of secret monitoring, search and seize.

---

302 Section 5 of the Privacy Protection Law.
304 Section 18(2) (b) of the Privacy Protection Law.
305 M.K.’s Akiva Nof and Shulamit Aloni raised this question in a debate of second and third reading, but their reservation was rejected, and noted in the Knesset Proceedings 20 (1980) 1769
307 Ibid.
308 Ibid.
2. Enforcement

Cybercrime is perceived by many as less serious than ordinary crime, both because hacking requires great sophistication and technological know-how, and because such crimes are perpetrated by people sitting in front of a screen and typing, and the damage that they cause is less concrete than damage caused by breaking into a bank strongbox for instance. Hackers in many places are considered cultural heroes and not criminals. However, cybercrime can have serious implications and requires special handling. Accordingly the Computers Law 1995 was promulgated.\(^{310}\)

This law is the result of the work of an inter-ministerial, interdisciplinary team appointed by the Minister of Justice and it unites within it several computer-related aspects.\(^{311}\) The need for legislation arose, inter alia, because of the unique nature of the computer and the central role that it occupies in our lives, the increase in cybercrime and the difficulties in adapting the existing laws to misuse of computers. Chapter 2 of the law allows handling of cyber-crime and thus – protection of abstract interests, which had no direct solution in legal provisions existing prior to this law. It should be noted that the use of the term “unlawful” in some of the sections of this chapter, means – transfer of the onus of proof to the prosecution.\(^{312}\)

In rulings that discussed this law, use was made in particular of two sections – section 2 (Disrupting or interfering with a computer or computer material) and section 4 (Unlawfully penetrating computer material):

In the **Refaeli case**,\(^ {313}\) it was decided that Refaeli transgressed sections 2 and 4 of the Computers Law. It was ruled that deletion of useless computer material is also a crime, and it is unnecessary to prove that the deletion caused damage or disruption to the computer.

In the **Badir case**,\(^ {314}\) the accused committed offenses through the automated telephone system, and were convicted of unlawful penetration of computer material. It was ruled

\(^{310}\) Computers Law, 1995.  
\(^{314}\) CF 40250/99 *Israel Police vs. Badir* (not yet published) (hereafter: Badir case). It was also established in the ruling that modern telephone switchboards are a computer as defined in the Law, and
that there is no need to prove damages for conviction of this offense. It was also established that it is not necessary for the penetration to involve expertise in computer operation and software: it is possible for the offense to be committed by an innocent agent, a person fooled into acting by the accused.

Ehud Tennenbaum, the “Analyzer”, was sentenced to six months’ community service and a fine of NIS 75,000 for hacking into the US Pentagon computers. It was ruled that he transgressed sections 2 and 4 of the Computers Law. The State appealed against the lightness of the sentence. In the notification of appeal (CA 71227/01), the State seeks to have a heavier sentence imposed on Tennenbaum out of considerations of deterrence. In its opinion the lightness of the sentence prejudices the deterrent and punitive message, and protection of public safety and security, in particular in a period in which there is a computer in every single field of modern life. The State also argues that a deterrent sentence is required as a kind of dam against the great temptation to commit cyber crimes, in light of the facility of committing them and the low probability of being caught.

Another difficulty in enforcement is that sometimes the offense is international – a person using servers located overseas, while the country in which he lives has only an incidental connection with the overseas servers. Section 140 of the Emergency Defense Regulations stipulates that a person disturbing a policemen or member of the government forces in fulfilling of his duty, commits a crime. Hackers penetrating government or army Internet sites can be convicted of this crime.

that penetration of a voice mailbox and listening to the messages left there, constitutes prohibited secret monitoring.

The ruling can be found at: http://www.law.co.il/computer-law/main.htm (14.2.02)
315Criminal Case (Kfar Saba) 3709/00 State of Israel vs. Ehud Tennenbaum, Tak. Shal. 3709 (2), 41.
316Boaz Guttman, “Averot Mahshev – Etgar Hadash” (Cyber-crimes – A New Challenge). A distinction between a computer offense (an action whose object is to prejudice the actual computer or computer network) and an offense in pursuance of the Prevention of Terror Ordinance (the computer serves as a tool for committing of the crime, for instance a Hamas activist managing activities of the members from an encrypted PC in the offices of an association masquerading as a Fund for the Needy). For a discussion of the difficulties of detection, prevention, enforcement and proof of computer crimes, in light of the nature of the Internet, At: http://www.psakdin.co.il/lp/public/art_bduc.htm (14.2.02)
317Defense Regulations (Emergency), 1945.
3. Search And Seizure

The search and seizure actions are legally permitted in order to protect state security interests and the right to life and in order to allow crime prevention and punishment. On the other hand, these actions are liable to prejudice the right to privacy and various economic interests of different organizations.

In the John Doe case, it was ruled that use of administrative arrest should be considered in light of the restrictive clause in the basic law: Human Dignity and Liberty. A balance must be found between defense of State security and the basic human right to freedom.

In the Public Committee Against Torture case, which dealt with the GSS investigator’s right to interrogate terror act suspects and with the physical means adopted against them, it was ruled that the violation of the liberty of the person interrogated would be allowed only if it was for a proper purpose and not beyond what is necessary, considering on the other hand the wish to protect the dignity and liberty of the person interrogated. As regards the requirement of immediacy, it will exist if there is a measure of concrete and real risk of occurrence of the event. (In the same case – in the event of a “ticking bomb”).

Search and seizure of material in computer systems

The Computers Law added to the definition of “belongings” in the Definitions section of the Criminal Procedure Ordinance (hereafter: CPO) also “computer material” and also added the definitions of “computer”, “computer material” and “output” to this Ordinance, as defined in the Computers Law. In the explanatory notes to the draft law it was explained, that the authorizations for penetration of a specific computer would be issued in pursuance of the search laws. Since the search provisions in the Criminal Procedure Ordinance did not include search of computer material, they were amended so that search of data or software on or belonging to a computer is also possible. Further an addition to Section 32 of the Criminal Procedure

---

318 CMC 3514/97, pp. 6/97 John Doe v. the State of Israel, Tak. Supr. 97 (2) 176, 177.
319 HCJ 5100/94, 4054/95 The Public Committee Against Torture v. the State of Israel, Decision 53 (4) 817.
320 The Public Committee Against Torture, ibid., pp. 834-835 (President Barak).
Ordinance (section 32(b)) was passed, whereby a court warrant is required for seizure of computer material of an institution. The reason – in order to prevent disruptions of the operation of the business or the public entity. A search and penetration to computer material warrant can be issued by a judge by virtue of sections 23 of the Criminal Procedure Ordinance (Search Warrants), 23a of the Criminal Procedure Ordinance (Penetration of Computer Material) and 43 of the Criminal Procedure Ordinance (Order to Obtain Article). Receipt of data from communications between computers by search will not be considered secret monitoring (section 32a(c) of the Criminal Procedure Ordinance).

In the Netvision v. IDF case, the court obliged the service provider to furnish the security forces with material collected in its computers and that was transmitted by e-mail of four of its customers. Netvision was required to furnish the said material by virtue of sections 23 and 43 of the Criminal Procedure Ordinance. When the State Attorney indicated that a warrant for seizure of e-mail in a service provider’s computers would be issued only by virtue of the wiretapping Law, the court indicated that an article seized by way of search without a lawful warrant is not inadmissible as evidence. Justice Even Ari indicated the decision delivered in the Nahmias Case, where President Barak ruled that “this new regulation comes to balance between the right to privacy and the infringement thereof: between inadmissibility of evidence and protection of the public interest.” Thus the court ruled that the material stored in Netvision’s computers could be seized even if the procedure that led to its storage was later found to be improper.

Other legal search and seize regulations

It might be possible to close an Internet site by virtue of section 5 of the Prevention of Terror Ordinance, which stipulates that any property of a terrorist organization, including property in the place of activity of the organization, in the possession of a member of the organization or that served for the organization’s activities, will be confiscated, and by virtue of section 6 of the ordinance that allows the Police Inspector General to close a place of activity of a terrorist organization.

---

322MC 090868/00 Netvision Ltd. v. Israel Defense Forces & others (not yet published), hereafter: Netvision case.
324Prevention of Terrorism Ordinance, 5708-1948.
Section 74 of the Emergency Defense Regulations,\(^{325}\) allows confiscation of articles when it is suspected that an offense was committed with regard to them or that they are liable to serve as proof of an offense, Section 99 allows seizure of any banned publication, sections 100-101 allow search of any device serving for printing and section 120 allows confiscation of the property of any person who transgressed these regulations.

Section 1 of the Legal Assistance Between States Law\(^ {326}\) defines an investigatory action also as search of premises and seizure of proof or an object (including computer material) and inspection thereof. Article 2(a) defines legal assistance, inter alia, also as search and seize actions, related to a civil or criminal case. In sections 29-30 there is an object seizure application procedure.

4. Secret Monitoring in Israeli Law

Modern technological development has placed on the agenda the legal questions deriving from development of wiretapping and surveillance means and from the ever-increasing use of electronic monitoring. The ease of use of listening devices, the unawareness of the injured party that his calls are being monitored, the difficulty of detecting existing monitoring and the limitation on protecting oneself against it led to the urgent need for solving of several of the problems deriving from secret monitoring.

A first secret monitoring draft law was submitted as early as 1962.\(^ {327}\) In the explanatory notes it was stated: “It is necessary to guarantee, by a criminal provision, that the privacy of the call will not be violated by secret monitoring.” The draft law did not become legislation and another draft law was formulated sixteen years later,\(^ {328}\) and this is the basis of the law promulgated by the Knesset.\(^ {329}\) The object of the draft law was to find the right balance between a person’s right to privacy and safeguarding of his privacy and the general right for protection by different ways, and inter alia by

---

\(^{325}\) Defense Regulations (Emergency), 1945.
\(^{326}\) Legal Assistance between States Law, 1998.
\(^{328}\) Penal Code Draft Law (Secret Monitoring), 1978, DL 5738/301.
use of modern technological wiretapping means. The law was designed to guarantee that invasion of a person’s privacy by carrying out of secret monitoring will be permitted only in cases where public-social interests take precedence over the right to privacy.

In formulating the wiretapping Law the legislators law based themselves on the American model in which there is an explicit distinction between secret monitoring which is prohibited, and monitoring and recording a call with the consent of one of the parties to the call, which is permitted. It was considered that if in the USA, the “bastion of safeguarding of the individual’s rights”, this perception does not constitute a criminal violation of the rights of the individual, then it should be applied also in Israel.

In pursuance of the wiretapping Law, monitoring of someone else’s call, recording or copying thereof, by a device and without the agreement of either of the parties to the call, is legally prohibited secret monitoring. Hence, if one of the parties to the call agreed to the wiretap, this is not secret monitoring. Monitoring of a call and recording of it for purposes of committing an offense or a damaging act, constitutes prohibited secret monitoring, even if one of the parties to the call give his consent. In the Zuberi case it was ruled that a man can be considered as a “party to a call” even if he only listens, provided that the other directs the message directly to the listener.

331 Knesset Proceedings 1975, 3974.
332 See definition of “monitoring” and “secret monitoring” in section 1 of the Secret Monitoring Law. For interpretation of the decision and definitions of “call”, “party to a call” and “call of others”, see: Chahnoever, supra, note 330, p. 591-596. In this affair the Supreme Court ruled “anyone who says things by a communications means that reaches or can reach the ears of many, makes all those who hear it parties to his call… When the person initiating the call says what he has to say in such a way that others can listen, he assumes the risk that others whom he did not intend to listen to the call will hear it. Like a person who shouts to his friend in public. He cannot expect his words to remain secret.”
333 In the explanatory notes to section 1 of the Penal Code Bill (Secret Monitoring ) 5738-1978, it was said: “It is proposed not to forbid monitoring of a call when one of the parties to the call agreed to this monitoring. The assumption is that the said consent removes the call from the definition as a call that was intended to be made personally only, and just as a person is liable to use his memory to reconstruct a conversation that he had with another, thus he can record it and could even ask someone else to do so. Section 3 of the Secret Monitoring Law.
335 CA 1497/92 Israel Police v. Zuberi, P.D 47 (4) 177, 193.
From this we may conclude that one area dealt with by the wiretapping Law is the actual prohibition of secret monitoring. In the additional area the Law restricts application of the prohibition, stipulating two exceptions: one exception relates to cases where monitoring is permitted a priori without need of authorization. When the call is made in the public domain, monitoring of it by a person authorized to listen, is not unlawful secret monitoring. While such monitoring requires authorization, the law does not stipulate concrete authorization. However, it seems that the authorization must be by name, must relate to a specific matter, and in as far as possible be restricted in time and place. The second exception applies to cases where permission will be accorded for secret monitoring that is not in the public domain. The law places more serious substantive and procedural obstacles before monitoring in the private domain. Secret monitoring as aforesaid will be allowed only for two purposes, for protection of state security or for prevention of crimes and detection of criminals. The authorization may be given only to a state authority: wiretapping for state security purposes can be executed with a written authorization from the Prime Minister, or the Minister of Defense, and in urgent cases with an authorization from the head of the General Security Service or the Head of the Intelligence Branch in the IDF General Staff. Secret monitoring for prevention of crimes and detection of criminals requires authorization from the President or Vice-President of the District Court. In urgent cases an authorization from the Israel Police Inspector-General suffices.

336 Section 8 of the Secret Monitoring Law. The “public domain” is defined as “a place where a reasonable person could expect his calls to be heard without his consent, and also a place in which a detainee or prisoner is held at that time”. Authorization to carry out such secret monitoring will be given by the head of a security authority for reasons of state security, or by a police officer for prevention of crimes and detection of criminals (Sections 8(1)(a) and (b) of the Secret Monitoring Law, respectively). For explanation of this concept see: CF 546/78 Bank Kupat Am Ltd. v. Hendels, P.D. 34 (3) 57; Rehearing of Civil Appeal 13/80 Hendels v. Bank Kupat Am, P.D. 35 (2) 785.


339 Ibid., at 533.

340 Definition of “Minister” in section 1 and Section 4 of the Secret Monitoring Law.

341 Definition of “Defense Authority” in section 1 and section 5 of the Secret Monitoring Law.

342 Definition of “Defense Authority” in section 1 and section 5 of the Secret Monitoring Law.
Wiretapping without a lawful authorization constitutes a criminal offense, for which a penal sanction can be imposed in pursuance of a provision of Section 2(a) of the wiretapping Law. The section sets down two further criminal offenses: use of information and placing of devices. Section 2(2) of the Protection of Privacy Law stipulates that “legally prohibited monitoring” constitutes an infringement of privacy. However, while secret monitoring constitutes a tort in pursuance of the Privacy Protection Law, it does not constitute a criminal offense by virtue of that law.

Proof obtained by secret monitoring, contrary to the provisions of the wiretapping Law, in general will be inadmissible in any judiciary procedure, unless the required conditions for admission of the evidence were fulfilled. Prior to amendment of the wiretapping Law in 1995, Section 13 constituted a mandatory provision that left no room for discretion of the court as regards admissibility of evidence. Today, the court may, in certain circumstances and according to its discretion, admit as evidence secret monitoring even if it was obtained unlawfully.


345 sections 2(b) and (c), respectively. On the parallel application of the Secret Monitoring Law and the Privacy Protection Law on these acts, see: on criminal and civil liability for one act, in pursuance of the Secret Monitoring Law and the Protection of Privacy Law, see Rosen, Ibid. at 160-162.

346 Privacy Protection Law. The widespread opinion today gives priority to the regulation stipulated in the Secret Monitoring Law over that stipulated in the Privacy Protection Law.

347 section 4 of the Privacy Protection Law stipulates that “infringement of privacy is a civil wrong...”. On criminal and civil liability for one act, in pursuance of the Secret Monitoring Law and the Protection of Privacy Law, see: Rosen, supra note 344, at 160-169.

348 section 5 of the Privacy Protection Law sets down a list of infringements of privacy that constitute a criminal offense, however it does not specify an alternative in pursuance of section 2 (2) of the Privacy Protection Law. Accordingly, in matters constituting secret monitoring legal action will not be taken in pursuance of the Privacy Protection Law. See for this matter Badir Case, supra note 314; Rosen, supra note 344, at 156-160.

349 section 13(a) of the Secret Monitoring Law.

350 The Secret Monitoring Law (Amendment), 1995. In the past section 13(a) of the Secret Monitoring Law included inadmissibility. The amendment of the provision of section 13 was designed to create checks and balances between the need to detect truth and do justice on one hand, and to prevent infringement of the rights of the individual on the other, giving discretion to the court to admit evidence even if it was obtained through transgression of the Secret Monitoring Law. See: The Secret Monitoring Draft Law (Amendment), 1994, DL 1994.

351 For the legal situation prior to amendment of the Secret Monitoring Law, see CA 2286/91 IP vs. Iluz, P.D 45 (4) 289, 304. For the legal situation after the amendment, see Nahmias case, supra note 323 above, pp. 325-326, 357-358.
Authorization for carrying out secret monitoring both for the purposes of state security and for prevention of offenses, is issued for a period not exceeding three months, and can be extended again.  Such an authorization would seem to contain serious infringement of privacy, even more serious than that deriving from a search warrant. While the search is carried out on a one-time basis and with the suspect’s knowledge, secret monitoring continues over time, is performed without the suspect’s knowledge and is even liable to infringe the privacy of innocent third parties.

The Court’s Role

Whereas it is the Legislator who established the desirable balance between the conflicting interests in the wiretapping Law, it is the Court’s role to deal with the work of interpretation of the law, and in the concrete implementation of the balance of interests. As already mentioned, secret monitoring for crime prevention requires a prior court authorization.

Implementation of the regulation in the wiretapping Law depends to a great extent on the way in which the courts have interpreted the expressions “in the public domain” and “in the private domain”. Verbal explanation of these expressions does not appear necessary; and the guiding policy considerations must adapt themselves to technological progress. An objective-proprietary distinction can be proposed, that determines that a private area, in which any person can enter and stay, is considered as the public domain. However, since the object of the wiretapping Law is to protect a person and not property, this distinction may be irrelevant. Therefore, a broader outlook should perhaps be preferred, that protects the privacy of a person and not the privacy of a place. A subjective criterion might also be proposed, based on the expectations of the parties.

From this we may conclude that technological progress in the communications market gives rise to legal doubts, and the court in its work must decide in borderline cases,

---

352 Sections 4(c) and 6(e) of the Secret Monitoring Law.
353 Section 6(a) of the Secret Monitoring Law.
354 The distinction is based on Stein’s article, supra note 338 above, at 533-535, 556.
355 Ibid., p. 533, 535.
basing itself on the existing legal regulation. However, it seems that changes occurring in technology lead, at the same time, to modification of the legal tools. Thus for instance, the wiretapping Law was amended in light of development of wireless communications.

The wiretapping Law initially defines a “call” as “by speech or another communication means”. Over the years the question arose as to whether monitoring of a call transmitted over the ether also comes within the area of the prohibition. Whereas in the not-so-distant past monitoring of a wireless telephone did not constitute an offense in pursuance of the wiretapping Law, today there is no longer any doubt that listening to a cellular telephone is subject to the regulation in the wiretapping Law.

In relation to the Internet age, when the wiretapping Law was promulgated, the legislator did not foresee the possibility of monitoring and tracing the individual by digital medium. This being so, what are the legal tools available to the court when it is required to decide on the question of monitoring and tracing in the digital medium?

A “call” is defined as including “communications between computers” Therefore, recording of information from communications between computers is monitoring, and in the absence of agreement of the parties to the call, this is secret monitoring, which constitutes a criminal offense. It should be noted that monitoring of communications between computers does not constitute “penetration of computer material” as indicated in Section 4 of the Computers Law.

---

356 See Chahnover case, note 330 above; see CA 5424/96 Israel Police v. Dov Tal, Tak. Supr. 96(3) 88; CA (Tel Aviv) 1770/97 State of Israel v. Laufer, Tak. Dis. 98 (2) 2377

357 See Secret Monitoring Draft Law (Amendment no. 3) (Prohibition on monitoring a wireless telephone call), 1994, DL 122; Secret Monitoring Draft Law (Amendment no. 4) (Prohibition on monitoring a wireless telephone call and increasing penalties), 5755-1994, DL 5755 123.

358 Section 2 of the Secret Monitoring Law establishes the legal liability of prohibited monitoring.

From the case law, the law is apparent: any use of communications means that allows access to the general public, is exposed to unauthorized monitoring, which is not prohibited by law. 360 This gives rise to the question of whether use of the Internet for purposes of conversation is exposed to tracing and monitoring in general, and by investigative and security agencies in particular? On one hand, the Internet users “expect safeguarding of their privacy”, and all the more so since the public Internet, which seeks to encourage free use of modern computer communications, obliges strict compliance with the provisions of the wiretapping Law. In this way the aim of the law will also be fulfilled. On the other hand, this curbing of the authorities from infringing the privacy of dialogue in the age of modern communication is not always possible, even if desirable, when in opposition another vital public interest might be violated.

Moreover, in the Badir Case it was determined362 that communication between computers includes, inter alia, communications to a voice mailbox, managed by computer. Hence, monitoring of a voice message on an answering machine, without the consent of the person leaving or receiving the message, is secret monitoring. Therefore, it seems that the protection of the wiretapping Law extends to methods of communication, but the secrecy of the conversation in itself is not protected.

In the Netvision case,363 the question arose as to what extent the investigator and security agencies are entitled to penetrate e-mail messages of an Israeli Internet

360 See Nimrod Kozlovski “Mishteret Ha-Internet” (The Internet Police), at: http://www.itpolicy.gov.il/topics/article_law2_karma_police.htm (last visit: 11.01.02). He argues that adopting of this sweeping law is undesirable, since it contains serious infringement of a man’s right to privacy, privacy in his life and confidentiality of his conversation. His proposal is to determine a criterion whereby, when the individual adopts real means to defend the secrecy of his dialogue on the Internet, a legitimate expectation of privacy is concluded from this, and this kind of dialogue should be considered as the “individual domain” and as such it should be protected from monitoring. Professor Stein in his article criticizes this objective-subjective test as regards the individual’s legitimate expectation, and explains why it should not be adopted in the framework of the Secret Monitoring Law. In his opinion, the limits of the individual domain should be fixed by objective evaluation of the effective and legal means of privacy adopted by the individual, with the aim of keeping his calls private. Objective criteria make clear the distinctions between the “individual domain” and the “public domain” and help the police investigators to carry out their work in pursuance of the Secret Monitoring Law. Stein, note 338 supra, at 532-539.
361 See the Netvision supra note 322.
362 See Badir supra note 314.
363 See the Netvision supra note 322.
subscriber, and whether they are entitled to oblige Internet access providers to carry out prolonged track and trace activities for purposes of the investigation. According to the current legal situation, as reflected also by the position of the State Attorney, e-mail that was already transmitted to the Internet access provider can be seized by order of a Magistrates Court, by virtue of the provisions of the Criminal Procedure Ordinance (Arrest and Search).\textsuperscript{364} As regards e-mail not yet transmitted to its destination, the seizure will be effected by an order of the President or Vice-President of the District Court by virtue of the wiretapping Law.\textsuperscript{365}

\textbf{The Territorial Application of the wiretapping Law}

In the \textit{El Mazri} case, it was ruled that secret monitoring outside the borders of the State of Israel do not have to be authorized by the President of the Court.\textsuperscript{366} In the \textit{Assaf} case,\textsuperscript{367} the High Court ruled on the lawfulness of monitoring calls between an inhabitant of southern Lebanon and an inhabitant of Israel when the monitoring was carried out simultaneously in Israel and in Lebanon. The appellant’s defense counsel argued that the wiretapping Law does not apply to southern Lebanon, and that in any case there is no court in Israel empowered to authorize secret monitoring of this kind.

It was ruled that the wiretapping Law does not require authorization for monitoring the call of both the parties to the call. It suffices to have an authorization to listen to one of them to in order for the monitoring to be allowed. Therefore, even if it was said that the monitoring of the telephone in Lebanon was inadmissible as evidence, it can be concluded that the monitoring of the telephone in Israel, in which the conversations of both parties to the call were recorded, are admissible as evidence.

\textsuperscript{364} Criminal Procedure Ordinance (Arrest and Search) [New Version], 1969, Laws 284.
\textsuperscript{365} Haim Ravia “Lo Yado Ha-aruka shel Hahok” (Not the long arm of the law) (June 2000). At: \url{http://www.law.co.il/hebarticles/2nv_v_idf.htm} (last visit: 12.01.02
\textsuperscript{366} CF 4211/91 \textit{Israel Police vs. El Mazri}, P.D 47 (5) 624. For criticism of the decision in the \textit{El Mazri} case, see: Yehonatan Ginat “Hatehula Hahutz-territorialit shel Zehuyot Ha-adam Ugevulotav shel Hok Ha’azanat Seter” (The extraterritorial application of human rights and the limits of the Secret Monitoring Law)42 \textit{Haperkalit} (1995) 518. The author considers that in light of the basic law: Man’s Dignity and Liberty, the correct interpretation of the Secret Monitoring Law is its application to every person wherever he is, whether he is on or outside Israeli territory. He argues that if the basic premise is protection of a person’s privacy, then the Secret Monitoring Law prohibits monitoring of a conversation in a place where the party of the call expects, and is entitled to expect privacy. This legitimate expectation does not disappear with the change of the place of the call. Hence, the criterion of the location of the communications means which is monitored should not take precedence over the criterion of infringement of privacy. Therefore the Secret Monitoring Law applies extraterritorially, and secret monitoring in the occupied territories requires a prior court authorization for carrying out of the monitoring.
\textsuperscript{367} CF 568/99 \textit{Assaf v. IP}, Tak. Supr. 2001 (2) 242, 246.
Mutual Assistance between Countries in Carrying Out Secret Monitoring

The object of the Legal Assistance between Countries Law is to regulate the different principles, methods and actions for granting of legal assistance by the State of Israel to other countries, and to regulate the provisions for applications by the State of Israel to another country for receipt of legal assistance.\textsuperscript{368}

Secret monitoring is included in the definition of “investigatory action”, which is listed among the actions that may be carried out in the framework of legal assistance.\textsuperscript{369} While the legal assistance regulated in the law is given both in civil and in criminal cases, the application of another country for secret monitoring in Israel, will be carried out only with regard to a criminal case. The competent authority in Israel will apply to a district court for authorization to carry out secret monitoring if one of the terms stipulated in section 31(2) of the Legal Assistance Between Countries Law exists.\textsuperscript{370} It may be said that application for legal assistance from a foreign country is not a routine matter, and appropriate arguments and reasons must be submitted as to why the court should accept the application lodged with it. The applicant must convince the court, inter alia, why the evidence is required for the procedure before the court, and why the applicant himself will not apply to the foreign country for the evidence, in particular in the case of available documents required in a civil procedure.\textsuperscript{371}

Secret Electronic Traces of Movements of People and Objects

The wiretapping Law does not protect the individual from electronic penetration and trace in the field of privacy in general, but is designed to protect the individual only

\textsuperscript{368} As indicated in the explanatory notes to the Legal Assistance Between Countries Draft Law 1997, DL 5957-1997 131.

\textsuperscript{369} See sections 1 and 2 of the Legal Assistance Between Countries Law. It should be noted that Section 5 of the Legal Assistance between Countries Law stipulates an escape provision, allowing refusal of the application of another country, if the legal assistance is liable to prejudice, inter alia, the security of the State of Israel or public welfare.

\textsuperscript{370} Authorization for secret monitoring will be granted only if requested for an offense, which in pursuance of the laws of the applicant country carries a sentence of over three years imprisonment; or in the case of an offense for which secret monitoring would be authorized if the offense was committed in Israel; or if the secret monitoring is for the purpose of confiscation of assets as stipulated in Section 6 of the Legal Assistance between Countries Law.

\textsuperscript{371} CMC (Jerusalem) 2168/99 \textbf{Prof. Malvina v. Dr. Wolf}, Tak. Dis. 99(3), 29742, 29743.
from penetration of his private calls.\textsuperscript{372} The Privacy Protection Law applies to electronic trace of a person’s movements.\textsuperscript{373}

The Privacy Protection Law also recognizes the needs of the defense authorities to act to safeguard social and public interests. However, in contrast to the wiretapping Law, the Privacy Protection Law does not include \textit{positive authorization} to carry out electronic tracking of a person’s movements,\textsuperscript{374} but authorizes infringement of privacy by way of giving an \textit{exemption} to the security and investigatory authorities, or persons employed by them, who acted “reasonably in the scope of their functions and for the purpose of their performance.”\textsuperscript{375}

The legality of infringement of a person’s privacy is examined according to reasonability of the electronic trace carried out with respect to him, and taking into account the legitimate aims of a criminal or security investigation.\textsuperscript{376} Material obtained in the framework of unlawful monitoring cannot serve as evidence in court, except with the injured party’s consent, unless the court authorized the use for reasons that will be recorded.\textsuperscript{377}

The question arises of whether the provision of section 2(1) of the Privacy Protection Law prohibits online tracking of the activities of Internet users? Surfing the Internet leaves “tracks” after the user, that allow creation of a personal profile concerning him. This increases the fear of infringement of the user’s right to privacy.\textsuperscript{378}

\textsuperscript{372} Stein, note 338 at 528-529.
\textsuperscript{373} The Privacy Protection Law defines infringement of privacy, inter alia, as “detection or tracking of a person, liable to harass him...” (section 2(1)). Section 5 of the Privacy Protection Law also stipulates that said infringement of privacy may be a criminal offense, in circumstances in which the public interest is prejudiced.
\textsuperscript{374} For a criticism see: Stein, supra note 338 at 555-556.
\textsuperscript{375} Section 19(b) of the Privacy Protection Law. It should be noted that the “balance formula” adopted by the Privacy Protection Law differs from and is more complex than that adopted by the Secret Monitoring Law, since it contains many more legally protected interests. For a more detailed context in this respect see: Rosen, supra note 344.
\textsuperscript{376} Stein, supra note 338 at 555.
\textsuperscript{377} Section 32 of the Privacy Protection Law
\textsuperscript{378} Haim Ravia “Pratiut Bareshet” (Privacy in the Internet) (four parts – Jan.-Feb. 1999). At: http://www.law.co.il/hebarticles/privacy1.htm (last visit: 12.01.02.)
5. Liability of Internet Service Providers

In Israeli law there is today no specific regulation either in legislation or in case law, as regards the question of ISP liability for the content or nature of the information published on servers. On the question of ISP liability for infringement of privacy, the opinion was expressed, in the context of Cookies, that everyone is aware of the infringement of his privacy through Cookies, but does not take any action to prevent the infringement, so the liability for the infringement of privacy cannot be placed on the ISP. It is inconceivable that the public will enjoy the advantages of the infringement of privacy through the Cookies, and on a parallel will demand financial compensation for the use of the Cookies. On the other hand, in the case of dissemination of defamation on an Internet site, the ISP must be obliged to divulge the identity of the distributor if so requested by the court, despite the infringement of privacy. This is because the ISP customers must be aware of the ISP’s duty to comply with court orders, and because it is inconceivable that distributors of harmful contents (e.g. defamation) should receive cover of legal protection preventing disclosure of their identity for reasons of privacy.

Possibly existing legislation in relation to cellular service providers and cable broadcast franchise-holders may enlighten us with regard to the appropriate law in relation to ISP liability. In pursuance of Section 13 of the Bezeq Law, 1982, a licensee for operation of Bezeq activities, for provision of Bezeq services or satellite transmissions, must allocate resources, as decided by the Minister of Defense or the Minister of Internal Security, to the security forces. Further, there are special articles in the license for carrying out of Bezeq services, which set down specific instructions in relation to the licensee’s obligation towards the defense system. In section 6(25) of the Bezeq Law there is a list of broadcasts which the license-holder for cable broadcasts or satellite broadcasts is forbidden to broadcast.

381 Bezeq Law, 1982.
382 For instance, in his lecture Adv. Sharon Keren of Cellcom noted that Section 48 of Cellcom’s license orders the absolute allocation of resources to the Defense System. Section 66a of the Cellcom license obliges the company to allocate special services to the Defense System.
We find that in actual practice the ISP confirm that they will keep digital evidence of committing of any offense, from the time of receipt of a request from the customer in respect of committing of the offense. This is done so that it can be presented to the police when so required. The existence of such a practice strengthens the need for legislative anchoring of ISP liability, both in order to impose on all the service providers identical liability and to prevent the phenomenon of the slippery slope.

F. The Information Age: Is there a Need for New Regulation

1. Is the existing system of checks and balances suited to the Internet?

Are the checks and balances between security needs and the rights of the individual that developed in relation to wiretapping and monitoring in analog communications suited to the Internet? To our mind, the new technology does not justify abandoning of the values that preceded it with regard to the balance between privacy and public interests of preventing terrorist activity. However, the legal regulation, both legislation and case law, must be formulated taking the technological characteristics into account. In particular, we wish to emphasize several unique characteristics of the Internet, of use of the Internet and of its users, which are liable to be relevant in the application of various balance formulae:

1. “Digital tracks” – as already noted, the Internet is an information environment in which all communications and message exchanges constitute in fact a type of data processing that creates a record. The monitoring possibilities are inherent and are effected routinely as part of the system operation. While as regard telephone calls a special wiretapping device must be installed in order to listen in to the call, on the Internet the contents of the conversation and identification of the means of the speaker and the addressee are recorded automatically. In many cases “monitoring” or recording will constitute a default, and the

---

383 As indicated by Mr. Ariel Pisetzky, CEO of Information Security at Netvision, at the Shefayim Conference.

384 The phenomenon of the slippery slope might occur if Netvision, for instance, because of its willingness to infringe the customer’s privacy by storing digital evidence, before being so required by the police, might be asked to carry out further infringements of privacy, without there being any legal base for them.
safeguarding of the privacy will require an active operation of deletion, canceling or prevention of the recording. Legally, this distinction is liable to have implications. For instance, the legal rule concerning telephone calls must determine the circumstances in which wiretapping can be carried out as is done in the wiretapping Law. The application of the formula of checks and balances in the Internet is liable to require definition of the circumstances that will oblige an operation of prevention, or deletion of existing files, or imposing restrictions on the uses, the distribution and the saving of this data.

2. The digital environment has very powerful invasive means, which in fact make the individual and his acts transparent (or potentially transparent) and are liable to create unprecedented infringement of privacy. These means allow penetration of the private domain. The computer connected to a global network creates in fact a kind of back door to the privacy of a person’s documents on the computer. Recently it was reported, that by means of software planted in a PC through the Internet it is possible to produce photographs of what happens physically in a person’s home. Further, monitoring software and databanks allow collection of information (by monitoring and cross-reference) of users in the public domain.

3. In the digital environment there is a considerable difference between the expectation of privacy and the invasive reality in which the individual is more exposed than in the past to invasion of his privacy. This fact can be attributed to several factors:

- Awareness of invasive means. The invasive means are not transparent to the user – these are a combination of software and hardware systems not visible to the end user, and understanding of the threat to privacy that they contain is liable to require above-average technological know-how and sophistication.

- The experience of surfing creates an illusion of privacy: It is done privately. In many cases the surfer is in his home or his office, the surfer is alone and not in public; surfing is an independent activity, on
the face of it, in cooperation with other people; interactive services are experienced in many cases as activity in the framework of a closed, intimate group. All these are naturally liable to increase the expectation of privacy.

- The frequent changes in the digital environment require routine updating of means and existing capacities of invasion of privacy: both in order to be aware of the threat and so that it will be possible to be protected against it.

Naturally it is possible to lessen the expectation of privacy and to warn the users of their exposure to monitoring means in the digital environment through education and information. On the other hand, the fact that the technology is still developing and changes at a dizzying pace is liable to reduce the effectiveness of these solutions.

2. What is the significance of implementation of the existing legal regulation to the Internet?

The existing legal regulation distinguishes between secret monitoring and search warrants as regards hardware, and therefore also relates to secret monitoring with greater strictness as regards the legal requirements. Secret monitoring that is regulated in the wiretapping Law protects the privacy of the dialogue, requires an order of the President or Vice-President of a district court, which will be issued in the conditions defined in the law. A search warrant, on the other hand, is in the jurisdiction of the Magistrate’s Court. Search and secret monitoring are distinguished from each other as regards awareness of the subject of the monitoring, the duration of the infringement, and the effect on third parties. In the case of a search, this is a one-time infringement, the person investigated is aware of it, and the infringement is focused on him and his belongings. Secret monitoring, on the other hand, is a prolonged infringement, without the knowledge of the person investigated, which is liable to violate the privacy of the suspect (in the framework of all the calls of the suspect which are monitored by the investigation agencies, personal communications of the suspect are also included which are not relevant to the investigation) and of third parties (other
users of the telephone lines, and parties conversing with the subject of the investigation).\textsuperscript{385}

In this context, what legal regulation should be applied to the Internet? **Monitoring on the Internet seems more like secret monitoring.** This is an action carried out without the knowledge of the subject of the investigation – at times with cooperation with the service provider only. This is prolonged activity, which is liable also to infringe the privacy of other surfers.

**G. Summary of Recommendations**

Our recommendations are based on the premise that the privacy of the surfers must be safeguarded, and that the extreme technological changes latent in the digital environment should not lessen the right to privacy or protection of privacy. However, the individual legal rules must be formulated, taking into account the special technological characteristics discussed above. The opposite is also true: values of privacy must be built into the technology.\textsuperscript{386} The absence of national frontiers on the Internet must also be taken into account,\textsuperscript{387} as well as the digital divide: the capacity (economic and technological) of surfers to handle the threat to their right to privacy differs. Therefore the public must be informed and educated as regards its right to privacy, the threats to this right, and the way to handle these threats.

Another difficulty is that alongside the public threat (from the State) to the right to privacy, there is in the digital environment a no less substantial threat to privacy – a threat deriving from commercial and private agencies. In this context, the question arises of the extent to which the State must be restricted in use of means that are accessible to every private agency? A separate discussion is required for the question of the relation between private regulation and public regulation. In this paper, we merely wish to point out the difficulties.

\textsuperscript{385} See lecture of Adv. Naava Ben Or, on p. 22 of the transcript of the afternoon session, Shefayim Conference (27.12.01).

\textsuperscript{386} See for instance the P3P technological standard at: [http://www.w3c.com](http://www.w3c.com), and also Lawrence Lessig, *Code and Other Law of Cyberspace* (N.Y. 1999).

IV. Online Propaganda: Security, Freedom of Speech and Service Providers’ Liability

A. What is “Terror Propaganda”?  
1. Terror Propaganda and Propaganda in the Service of Terror  

Some see terror as a type of communications. Namely, transmitting of a message by actions rather than by words. In this sense terror in itself constitutes propaganda. Groups and organizations that carry out violent acts in order to further political objects, create the terrorization and intimidation effect by communications. The communications effect of the acts of violence creates the terror effect of those violent acts. Terrorist organizations depend on the publicity given to them. Without it they cannot exist. In this sense symbiotic relations exist between terror and the media. These relations are expressed in the fact that the media provides the terrorist organizations with their “oxygen”; without publicity and advertising their struggle would have no value. Likewise the various communications channels compete constantly for the market sectors required for an information provider, and excitement. They are therefore bound to play easily into the hands of terrorist organizations that provide abundant drama, and are liable to disseminate their propaganda unknowingly. Therefore, the more the mass media develop and spread, and through them the coverage given to the different terrorist organizations grows, the more the potential for terror acts grows. This aspect naturally raises dilemmas regarding the scope and nature of media coverage of terror attacks, dilemmas that are exceed the scope of this paper.

However direct propaganda also constitutes a main part of the activity of terrorist organizations. “Terror Propaganda” or psychological warfare (PsyWar for short) is an attempt to create a convenient reality through influence on conscious and unconscious positions of the adversary. The objects of the propaganda are liable to be diversified. Sometimes their aim is to sow fear and to deter populations. The rationale is that if the


389 To quote Margaret Thatcher, the terrorist organizations hunger for the “oxygen of publicity”.

139
enemy is afraid, it will be easier to vanquish him. “Smart” psychological warfare attacks the adversary’s credo, outlooks and values. For psychological warfare to succeed, it is necessary to know and understand the opinions and values “professed by the “enemy”. This chapter will deal with questions relating to propaganda in the service of terror. The more sophisticated and consolidated the terrorist organization is, the greater will be its use of psychological warfare. Terror Propaganda uses the freedom of speech given to the mass media, in order to transmit its harmful messages. The free communications in Western society are extremely vulnerable to exploitation and manipulation by terrorist organizations. Terrorist organizations see the free communications as an effective and convenient tool, which they exploit cynically, even while despising and combating democratic values. Terror Propaganda uses democratic values, and above all freedom of speech, to trap the government authorities, so that they will be obliged to grow accustomed to the propaganda published or to censure the communications, thereby incurring public criticism.

The terrorist organizations use propaganda to further four main objectives:

1. Dissemination of propaganda and sowing fear and terror in the “target group”.
2. Mobilizing as extensive as possible support for their struggle in the local population and world opinion. They do this by presenting justification of their object and describing their inevitable victory.
3. Distortion of the government responses, for instance by presenting government actions against terrorists as tyrannical and ineffective means.
4. Mobilizing activists and using them in information campaigns, recruiting of supporters and fundraising.

2. Contents of the Propaganda

At the information level, a distinction should be made between the propaganda directed at different target populations. The propaganda of the terrorist organizations is directed at potential supporters, towards the local public that is part of the “enemy”.

---

392 Wilkinson, supra note 392.
394 Wilkinson, supra note 392.
and towards the international community. The contents of the propaganda will of course be influenced by the target population. In this context a distinction is generally made between two aspects of propaganda.\textsuperscript{395}

The first, the \textbf{“hard” aspect}, relates to creating negative opinions in the public about the state, the government, society, etc. The aim is to create alienation between the public and the State. The way in which terrorist organizations do this is through presenting their “opponents” as the personification of evil. Since the enemy is so corrupt, they are obligated, so they will say, to annihilate it.\textsuperscript{396}

The second, the \textbf{“soft” aspect}, relates to creating a positive opinion and support in the group or organization leading the struggle. Here the object is to encourage people to support the organization and even join it. The way to do so is by persuading people, young people in particular, to assume the values of the organization and its method of activity or to identify with it. For the most part, the terrorist organizations emphasize the justice of their object, which is based generally on some secular ideology. They do not present themselves as “terrorists” carrying out acts of terror, but as “freedom fighters” with justified object and means. The terrorist organizations will generally play down their violent activity for information and image considerations, but will present the activity of the government using terms such as: massacre, murder and genocide. The terrorist organizations present themselves as persecuted innocents whose freedom of speech is curtailed and whose supporters are arrested by the authorities, all this as part of their psychological warfare. The object is to undermine the legitimacy of the existing government, and thus to place all the blame for use of violence on their opponents. Another rhetoric used by the terrorist organizations in order to create a positive opinion about them is the rhetoric of peace and non-violence, even though these are, as already noted, violent organizations. Most of the organizations will argue in their propaganda that they wish for a peaceful solution.


\textsuperscript{396} The sites of Hizbullah and Hamas, for instance, focus on presenting Israeli activity as terrorist activity. Presenting the enemy in this way is designed to justify the use of violence and harming of the innocent. Similarly, The Colombian National Liberation Army at its site indicates that the violence carried out by the organization is a result of the violence prevailing in the world and not the cause of this reality. See Zefati & Weiman, “Terror Be-Internet”, supra note 393, pp. 48-49.
3. Propaganda Methods
The standard methods of propaganda are through: pamphlets, books, radio and TV, fax, and recently also through the Internet. Until World War II most propaganda was conducted through printed leaflets. During the war the use of radio grew as a propaganda means. The use of TV as a propaganda means began in the 1960s, mainly during the Vietnam War. Use was made of propaganda also during the Cold War, with extensive recourse to journalists, authors and publishing houses.

Pamphlets, books, radio broadcasts, telephone, fax and the Internet serve mainly the “hard” aspect of the propaganda, creating alienation between the citizens and the State, but they have almost no influence on the “soft” aspect designed, as noted, to create identification with the said organization. The value of TV to the terrorist is expressed in that it also serves the “soft” sides of the propaganda.\(^{397}\) Publication of pictures or short clips by Internet can also serve this side of the propaganda.

4. Does the Medium Change the Nature? Psychological Warfare in the Technological age
The objects of terrorist organizations remain the same, also in the digital environment. However, the medium offers new possibilities, and its characteristics are bound to have implications for the status of the speakers, the messages, the measure of effectiveness etc., and thus for the legal treatment thereof. The question is therefore to what extent the use made by terrorist organizations of the Internet for propaganda needs differs from the uses made of other media, and to what extent it therefore requires different legal handling?

There are several characteristics of the digital medium that must be considered. The characteristics presented below do not constitute an exhaustive list, but reflect special aspects of the digital medium. It should be noted that there may be some overlapping, and in any case they should be seen as a whole.

- **Interactivity**: The Internet, unlike the conventional media, allows interactive relations between the organization and surfer's. The Internet

\(^{397}\) Raman, supra note 395.
user therefore has an effective means of running activists, and managing their activity. For instance, in addition to the propaganda published on the actual web site, many terrorist sites offer surfers to purchase books, videotapes and audiotapes, stickers, T-shirts and emblems of the organization.\textsuperscript{398} All these also constitute propaganda means. Naturally, such activity is not possible in traditional mass media.

- **Targeting the message**: Interactivity can allow the terrorist organization to target the message. Psychological warfare that used the mass media targeted a general public or an unspecified group of people. The Internet, on the other hand, makes it possible to select a small target population out of the community and to direct the propaganda only at this population. Different messages can be customized for different communities (world opinion, potential members of the organization, etc.) Therefore, the use of the Internet is likely to be more effective from the terrorist’s viewpoint.

- **Globalization**: The fact that this is a global network, accessible to everyone around the world, allows terrorist organizations to reach other publics outside the region in which they work. This is liable to constitute a tremendous information advantage, alongside the operational advantage, allowing recruitment and activation of activists outside the territorial borders.

- **Accessibility and availability**: Propaganda on the Internet can be carried out at relatively low costs: sending e-mail, setting up a web site. It is also possible at relatively low cost to set up a site disseminating the propaganda messages.

- **Independence**: Unlike advertising in the mass media, which is managed centrally by publishers who operating editing and contents control mechanisms, anyone can express himself on the Internet. Existing interactive systems can be used, e.g., chartrooms and forums managed by the Internet provider or the site operator. It should be noted that while a terrorist organization, which seeks to transmit a message in the mass media will use acts of terror in order to receive media exposure, the accessibility of the Internet makes this superfluous.

\textsuperscript{398} Zefati & Weiman, “Terror Be-Internet”, supra note 393, pp. 53.
• **A smaller public?** Despite the fact that the Internet is accessible to any spokesman without any censorship, filtering or editing system, and at low cost, it has disadvantages for the terrorist spokesman: the propaganda messages are liable to be swallowed up in the “data smog” existing on the Internet,\(^3^9^9\) and not to stand at the center of public attention, unlike the situation in which the mass media establish the public agenda. Further, in comparison to the mass media (such as radio and TV) the penetration percentages of the Internet are relatively low in the general public. Moreover, surfing the net requires a relatively higher level of reading skills than that required of the TV viewer, as well as financial means. In other words, the digital divide means that the potential target population of the terrorist who wishes to use the Internet is smaller and more sophisticated.

• **Legitimacy:** Some of the characteristics listed above, and in particular interactivity, accessibility and independence, allow the terrorist organization not only to transmit the message, but also to receive greater legitimacy than it could have obtained through traditional media. On the Internet, the terrorist organization is a speaker, and its status as speaker is identical, at least at the starting point, to that of an online journal, a commercial site, or any legitimate political organization. This is sound to the expressed for instance in the URL, or in the links to other sites. In the main the links are to sites with an ideology close to that of the organization or other sites related to the actual organization. Links can even be found to sites of human rights organizations.\(^4^0^0\) Links of this kind might create an impression of cooperation, patronage or other support. In this way, the terrorist-speaker exploits the advantages of the medium to obtain legitimacy.

### B. Freedom of Speech on the Internet

At first glance, propaganda of a terrorist organization is an integral part of the terror activity, and this gives rise to the public need to prevent it in as far as possible. The methods of fighting terror are varied, and any way in which we can fight it serves the

\(^3^9^9\) See: David Shenk, *Data Smog* (New York 1997).

\(^4^0^0\) Zefati & Weiman, “Terror Be-Internet”.supra note 393, at 57.
public: just as the law prohibits fundraising for a terrorist organization, membership in it, and of course prevention of the actual terrorist activity, so the law must also place obstacles in the way of dissemination of the propaganda by these organizations. However, propaganda has another aspect: it constitutes a form of speech. Therefore, the question of the legal response to terrorist activity on the Internet must also be examined from the perspective of freedom of speech.

Within the discussion of freedom of speech, it is first necessary to clarify what the protected interest actually is. Obviously the concern is not with the fate of the terrorist’s right to free speech, but with the fate of the public interest to know, or as this interest is generally called, “the public right to know”. Indeed, it is not always clear to us what the great benefit for us is of disclosure of the terrorist’s speech. Possibly, in many cases this is of no benefit to the public. However, the principle of freedom of speech assumes that exposure to another opinion, even a mendacious opinion, has an advantage: it strengthens the counter expression, challenges the “truth”, exposes the “true face” of the adversary, and obliges us to reexamine our positions. In any case, the accepted justifications of freedom of speech assume that it is not the State’s role to interfere and to restrict the access to speech.

Questions concerning freedom of speech are not new to Israeli law. The right to freedom of speech is not explicitly enumerated in the Basic Laws. However, it is considered a basic human right, and several justices have noted in decisions that it must be understood in the Basic Law: Human Dignity and Liberty. In Israeli case law an extensive doctrine has been developed in this area, constructed around checks and balances between freedom of speech and other rights (for instance the right to

---

401 This is based on John Stuart Mill’s theory of truth as justification for freedom of speech. However similar conclusions can also be reached according to other justifications. For a discussion of the theoretical basis of freedom of speech, see Ilana Dayan Orbach, “Hamodel Hademocrati shel Hofesh Habitui” (The Democratic Model of Freedom of Speech), Iyunei Mishpat (1997) 377; Guy Pesah, “Habasis Haiyuni shel Hofesh Habitui Umaamada Hamishpati shel Ha-itonut” (The Theoretical Basis of Freedom of Speech and the Legal Status of the Press), Mishpatim (2001) 895.


403 HCJ 2481/93 Dayan v. Jerusalem District Commander, P.D 48(2) 456, 468; CA 4463/94 Golan v. Prisons Service, P.D 50(4) 136, 158.
one's reputation). In these cases a “horizontal balance” is generally implemented. Or checks and balances between other public interests, for instance the public welfare, public order etc. (when a “vertical balance” is implemented). These balances, the most common of which is the criterion of “near certainty” relate to the possibility of restricting the speaker’s utterances. They were developed taking into account the technological characteristics of the media. For instance, one of the accepted justifications for interference in the contents of the broadcasting of radio and TV channels transmitting their broadcasts through the electromagnetic spectrum, is that this is a public and scarce resource.

Therefore the question is the application of the balances developed in case law to the new medium. One position argues that the balance is basically moral, is not technology-dependent, and therefore the new medium does not need to modify the fundamental attitude of justice to the problem arising. Another position states the opposite. It maintains that not only should the existing rules not be applied to the digital medium, but the new medium calls for reexamination of the principles of the existing checks and balances. According to this approach, legal interference in freedom of speech should be greatly reduced (even to the point of disappearing), also in the traditional media. An intermediate position argues that the different technology calls for a legal modification, but this does not have to be dramatic. The legal rules should be formulated according to the same principles and values that we held until now, but they should be adapted to the new medium according to its unique characteristics.

---

404 See for instance CA 214/89 Avneri v. Shapira, P.D 43(3) 840.
406 For further discussion of the subject of criteria developed by the court in the question of whether speech comes into the framework of offenses, which prohibit expressions of various kinds, see Elon Harel, “Averot Hamagbilot et Hoftesh Habaitui Umivhan “Efsharut Hahitmatamashut shel Nezek: Hashiva Mehudeshet” (Offenses that restrict freedom of speech and the criterion of possibility of realization of damages: reconsideration”) 30 Mishpatim (1999), 69.
408 For a fundamental discussion see Yuval Karniel, “Hoftesh Habaitui ba-Internet”, (Freedom of Expression on the Internet)1 Alei Mishpat (2000) 163.
409 For an argument in this vein, see Ariel Bendor, “Hasdara Mishpatit shel Ha-Internet le-ahar Iruei ha-11 be-September – bein Metziut Lemishpat” (Legal regulation of the Internet after the Events of September 11 – between Reality and Law)6 Mishpat Umimshal (forthcoming).
410 For this position, see Alon Harel, “Internet veHofesh Habaitui: Hirhurim mehudashim al Haregulatzia shel Bitui be-Eidan ha-Internet” (Internet and Freedom of Speech: New Thoughts on Regulation of Expression in the Age of the Internet).
characteristics. The advocates of this position emphasize mainly that on the Internet there is no problem of scarcity (unlike the electromagnetic spectrum). Further, regulation of expression on the Internet involves new costs, because of the “democratic” possibilities latent in the Internet: the accessibility is greater, the cost of expression is less, and there are possibilities of interactive expression: The surfer is not only a passive consumer of the expression, but also has the possibility of participating actively in the expression in the mass medium. Regulation, even if its aim is legitimate, is bound to prejudice all these. Existing law appears to tend towards the last mentioned position: the starting point in formulating the legal rules is that of the existing value balances, but in their application to the Internet attention must be paid to its special characteristics, and to the possible implications of such application: Justice Mishael Cheshin, in his capacity of Chairman of the Central Elections Committee, ruled that the restrictions in the Law on Propaganda Methods should not be extended to speech of a politician in an Internet chat room. His reasoning was based, inter alia, on the special characteristics of the Internet and on the importance of freedom of speech.

In the context of the Internet another question arises because of the technological characteristics: The speaker is able to express himself as a result of activity by various third parties, such as site storage service providers, managers of sites and online forums etc. It is therefore necessary to consolidate a position vis-à-vis their liability: is it possible to make them liable for the expression whose existence they make possible (indirect liability)? Should this be done? What are the implications if such a policy were determined?

C. Liability of providers

In cases in which there is a public interest that justifies restriction of the expression of the terrorist organization and the public right to know, the question is how this interest can be realized. Clearly, there is a practical difficulty in restricting the speech of the

---

411 For a comparison between the characteristics of the existing technologies and the characteristics of the Internet, see: 

412 See Election case 16/2001 Shas – World Union of Torah Observant Sephardim v. M.K. Ophir Pines, Deputy Chairman of the Central Elections Committee (decision of the Chairman of the Central Elections Committee (30.1.01)).
actual terrorist organizations, since they are not within the country’s borders and in any case (even if they do work within its borders), they do not obey the law. Therefore, quite naturally, attention was turned to various intermediate agencies that enable the terrorist organizations, by their very activity, to disseminate their messages on their sites (hereafter: “terrorist sites”). For instance, an Internet provider that hosts on its servers the sites of the terrorist organization, a provider that allows subscribers access to such sites (whether they are hosted on its servers or not), web sites that create links to terrorist sites, sites that offer interactive services (forums, chat rooms and so forth), etc. These mediators in fact constitute a kind of technical “bottleneck”: they are a convenient point at which it is possible to curtail the scope of the terrorist organizations’ propaganda activity. This leads to the question of the liability of these intermediate agencies.

The question of the liability of the different service providers is not exclusive to terrorist “speech”: it arose in the context of other harmful expressions, such as defamation, infringement of copyright, dissemination of pornography, and infringement of privacy. The experience accrued until now shows that alongside the wish to prevent and curtail harmful expressions, there are other considerations related to the structure of the public dialogue on the Internet, to the functioning of the market etc. We will first review the various considerations in the question of placing the liability on the Internet providers: what are the advantages of such a rule and what are its implications? We will then present the legal models developed in this context. Subsequently we will review the legal situation in Israel – and its uncertainty. We will conclude with our recommendations.

1. Considerations in placing liability on intermediate service providers

As already noted, the difficulty in identifying, locating and enforcing the law on terrorist organization leads us to the intermediaries. In other words, the main motive behind the norm of imposing liability on the intermediaries is the wish to certain protected interests, and here, the public interest in preventing activity that supports terror. Imposing liability on the providers has several advantages in this context:
• It is easier to locate a service provider than the individual end user who disseminated the terrorist propaganda.\footnote{Zefati & Weiman, “Terror Be-Internet”, supra note 394, at 58.} The provider conducts its business openly, over time, it has a physical and business presence and financial and legal activity that can be located easily.

• In the technological age the problems of locating the original speaker are growing, and it is not at all clear how it is possible to apply and enforce local laws on propaganda terror disseminated on the Internet, which is a global network. An example of this problem can be seen in the LICRA v. Yahoo! case. In this case the French court ruled that Yahoo! must comply with French law that forbids dissemination of Nazi items on the Internet, and therefore it must block access of the surfers in France to sites in which such items are offered for sale.\footnote{See League Against Racism and Antisemitism (LICRA) v. Yahoo! Inc., Yahoo! France(County Court, Paris, 20.11.00). \url{http://www.lapres.net/html/yahen11.html}. An American court ruled that Yahoo! does not have to comply with the French order. Yahoo!, Inc., v. La Ligue Contre le Racisme et L’antisemitisme, 169 F.Supp.2d 1181 (N.D. Cal., 2001).}

• Indeed most anti-regime organizations generally work outside the country against which their actions are directed. The solution to this problem lies in creation of international treaties. However this solution too is not simple, since it is not at all clear that what one country sees as “terror propaganda” will be seen as such by another country.

• Imposing of liability on intermediaries allows not only enforcement a posteriori, but also prevention a priori: Imposing liability creates an incentive to the service provider to screen contents before their publication, and in this way to prevent dissemination of contents that might comport a risk for it of legal liability.

• To complete the picture, in the broad context of imposing liability on intermediate agencies for harmful contents deriving from users, there is another consideration: Instead of all the damage falling on the shoulders of a single injured party, imposing liability on the provider allows compensation of the injured party. This principle transfers the damage, in the first stage, to the provider, which is generally a “deep pocket”. Usually, it is to be assumed that the provider will pass the cost on to its consumer public: In such a way, the damage will be dispersed among surfers, by
subscriber fees. This aspect is less relevant to situations of preventing terror, since the main object is to prevent the damage in advance and not to pay compensation afterwards.

However, alongside these advantages, of imposing liability on service providers, there may be undesirable implications:

- Imposing liability on service providers will oblige them to take a series of measures to avoid liability (for instance creation of a control and surveillance mechanism) or in order to protect themselves from it (for instance by legal advice or, in the civil context, purchase of insurance). These means have a high financial cost.

- Imposing the costs on the service provider actually means that only the provider’s subscribers, namely, the surfers, will bear the cost of the fight against terror – and not the general tax-paying public.

- Another anticipated implication is the raising of prices of the Internet services. The result is a further burden on the vital operations taking place in the digital medium: research, development, education, commerce, etc. In light of the digital divide in society, and the competition at the international level, this further burden has a serious implication.

- The legal and economic exposure creates an incentive among service providers not to provide interactive services, when operation of such services involves a risk. In these services the provider is not the source of the contents, and therefore does not control the contents disseminated by the surfers. On the other hand, these services constitute the source of the Internet’s force and contain many economic and democratic possibilities.

- Imposing liability has an immediate implication for freedom of speech: the provider fears that liability will be placed on him and therefore, in cases of doubt, will prefer to prevent a surfer’s advertising or activity. The service provider will therefore tend to operate “private censorship”. In this way the vital “oxygen” of freedom of speech will be prejudiced.

- In fact, this is privatization of the enforcement system. The service provider’s considerations in the control and surveillance that it will operate will be economic cost-benefit considerations. Clearly these are legitimate
considerations from the provider’s viewpoint. However, these considerations will actually replace the complex checks and balances developed in case law, checks and balances designed to protect human rights on one hand, and to guarantee the public interest on the other. Moreover, the provider’s discretion is not subject to the rules of administrative and constitutional law, the provider is not elected, and is not accountable to the public as regards the method of operation and the contents of its discretion.

2. Models for Liability of Intermediate Agencies
Existing legislative models can be classified into three main types: liability at one end, immunity at the other end and in the middle –conditional and restricted immunity, arising in certain conditions. It will be noted that in Europe a uniform regulation was adopted applying to all types of infringements and damages, while the American regulation establishes different legal regulations according to the types of damages and infringements – depending on whether their origin is in defamation, infringement of copyrights or another field.\(^{415}\) It should be emphasized that these models developed in the framework of civil law: in situations where an individual was injured, sought to prevent continued injury and to receive financial compensation for the damage caused to him, because of the contents published on the Internet by some other party. Accordingly, great caution should be used in adopting an analogy from this field to the public-criminal field of preventing terrorism. The standard of liability in the criminal context is higher: it requires proof of criminal intent beyond probable doubt.

a. Liability
One possible model establishes that the intermediaries are liable for the various activities carried out through them. This model exists, for instance, in the civil legislation that imposes liability not only on the direct infringer, but also on other parties, which indirectly assist the infringer. For instance, in the Defamation Law 1965 liability is imposed not only on the defamer but also on the “editor of the

\(^{415}\) For a comparative discussion, see: Kamiel Koelman, Bernt Hugenholtz, “Online Service Provider Liability for Copyright Infringement” ,WIPO Workshop on Service Provider Liability (Geneva, 1999).
media”, “responsible of the media”, “printer and distributor”. Likewise, copyright law imposes liability in specific situations on managers of banquet halls for playing of musical works, without a license, by disc jockeys. In American Law too, alongside the direct liability for infringement of copyrights indirect liability is also recognized, in pursuance of two legal doctrines: contributory infringement and vicarious liability. It will be noted that in Israeli law the doctrine of “joint wrongdoers” has long existed, and recently the court also recognized the tort of contributory infringement, at least in the context of patent laws.

b. Full Immunity

Another model, at the other end of the spectrum, gives full immunity to the intermediate agency. This approach is manifest in section 230 of the American Communications Law of 1996, which gives immunity to interactive service providers for liability for contents deriving from another:

No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

It will be noted that American Law distinguishes between publisher, which has absolute liability, and distributor, who is liable if he knew, or if he should have known of the damage/infringement caused by third parties. According to its wording, section 230 grants immunity from absolute liability only. However, this section was

---


417 See Sections 2(1)-(2)(3) of the Copyright Law, 1911 and also CF (Tel Aviv) 46/94 AKUM – Association of Music Composers, Writers and Publishers in Israel Ltd. v. Y.T. Gazit Jerusalem Ltd., Tak. Shal. 97(4) 1371; CF (Tel Aviv) 25/98 Israeli Federation for Records and Tapes Ltd. v. Atlantis Nesher Ltd., Tak. Dis. 98(1) 2668; CA (Tel Aviv) AKUM – Association of Music Composers, Writers and Publishers in Israel Ltd. v. Haan Hadekel Halls Ltd., Tak. Dis. 99 (1) 2144.


419 See section 12 of the Ordinance on Torts [New Version].

420 See CA 1636/98 Rav Bareah Ltd. v. Beit Mishar Leavizarei Rekhev Habashosh Ltd., P.D 55 (5) 337.

interpreted at length by the courts in the USA, and it was established that the service providers are immune in any case, even if they were given notice of the damage/infringement.\textsuperscript{422}

c. Conditional and Restricted Liability

Between the two models described until now, lies an intermediate model. According to this model, the provider will be exempt from liability in relation to certain actions provided that it met certain requirements established in the law. For instance, American copyright law establishes a detailed exemption regulation, dependent on three types of conditions.\textsuperscript{423} The first condition relates to the \textit{nature of the provider}: it must be an online service provider, as defined there.\textsuperscript{424} The second condition relates to the \textit{type of activities}: the immunity will apply only to the activities listed there: transmission and channeling of content in the system,\textsuperscript{425} temporary storing during transmission (use of caching),\textsuperscript{426} storage\textsuperscript{427} and links.\textsuperscript{428} The third condition defines \textit{requirements} that the provider must meet in order to receive immunity, and in particular, appointment of an “ombudsman”,\textsuperscript{429} and adopting a policy of "notice and take down", which means immediate removal of the infringing material, on receipt of a complaint,\textsuperscript{430} adopting of an enforcement policy, and the provider is required not to prevent parties from carrying out technological surveillance means.\textsuperscript{431}

\begin{flushright}
\textsuperscript{422} See Zeran v. America Online, Inc., 129 F.3d 327 (4th Cir. 1997). In that case information was disseminated at AOL (site and provider) about someone, stating that he supported blowing up of the Federal building in Oklahoma and was selling T-shirts with an inscription expressing his support. The person in question informed AOL that this was a lie, but AOL did not take the trouble to remove the advertisement from the Internet, an omission that led to his action against AOL. The court ruled that Congress’s object was to provide broad protection to the ISPs and therefore the term “publisher” must be interpreted in a broad sense in 47 U.S.C. §230(c) and for this case it must also include the meaning of distributor. Namely: the liability of publisher or of distributor will not apply to the ISP. In other words, the law gave the Internet providers immunity from damage claims by anyone injured because of publication of defamation and the like against him. Likewise, the immunity is granted to the provider also vis-à-vis the publisher, for acts of self-censorship that the service provider carried out. The decision expresses the customary law in the USA in this question. For criticism, see the minority opinion in Doe v. American Online, Inc, 783 So.2d 1010 (S.Ct. Fla. 2001).
\textsuperscript{423} 17 U.S.C. §512.
\textsuperscript{424} 17 U.S.C. §512(k).
\textsuperscript{425} 17 U.S.C. §512(a).
\textsuperscript{426} 17 U.S.C. §512(b).
\textsuperscript{427} 17 U.S.C. §512(c).
\textsuperscript{428} 17 U.S.C. §512(d).
\textsuperscript{429} 17 U.S.C. §512(c)(2).
\textsuperscript{430} 17 U.S.C. §512(g).
\textsuperscript{431} 17 U.S.C. §512(i).
\end{flushright}
The rule adopted in the European Directive as regards e-commerce establishes also an exemption from liability for certain actions, when the conditions listed there are fulfilled, as regards each of the actions benefiting from immunity.\textsuperscript{432}

3. The Legal Situation In Israel

In Israel the existing law does not explicitly regulate the liability of ISPs for harmful or forbidden content of third parties. In specific fields, liability applies to traditional intermediaries (that are not Internet providers) either by virtue of explicit legal provisions (for instance, the Copyright Law), or by virtue of case law (for instance patent law). The existing legal situation is this question therefore is unclear and one may well wonder at the constitutionality of some of the existing regulations.\textsuperscript{433}

In Israeli law there is a series of prohibitions on terror acts,\textsuperscript{434} and also on indirect assistance to terror acts,\textsuperscript{435} but the application of these prohibitions to the digital medium is not self-evident. For instance, there is in the Defense Regulations (Emergency) 1945 an obligation of censorship, i.e. of prior submission, for the authorization of the military censor, of information intended for publication.\textsuperscript{436} The law defines the term “publication” very broadly, and includes inter alia “to distribute, disseminate, deliver, announce, or make available to all persons.”\textsuperscript{437} It is not clear whether an Internet site on which a forum is conducted will be liable, in accordance with this definition, for offenses committed by the surfers participating in the forum. Likewise, a provider who allows access to terrorist sites. Another prohibition in the Regulations is provision of printing services to a banned association.\textsuperscript{438} Again, here too it is unclear whether this section is applicable to Internet sites.

\textsuperscript{434} See in particular Prevention of Terrorism Ordinance, 1948.
\textsuperscript{435} See for instance Defense Regulations (Emergency), 1945, in particular sections 58, 66.
\textsuperscript{436} See sections 87, 96 of the Defense Regulations (Emergency), 1945.
\textsuperscript{437} See section 86 of the Defense Regulations (Emergency), 1945.
\textsuperscript{438} For a discussion see CF 538/89 Warshavski v. Israel Police, P.D 44(2), 870 (the printing press printed Popular Front training brochures. The appellant was convicted of an offense in pursuance of Regulation 85(1)(g) of the Defense Regulations (Emergency), 1945).
The Prevention of Terror Ordinance 1948 reflects the policy that the fight against terror calls for a fight against accompanying infrastructures. For instance section 1 of the Ordinance defines membership in a terrorist organizations broadly, including also anyone publishing propaganda for the organization; section 2 includes in definition of “activity of a terrorist organization”, inter alia, a propaganda speech at a public meeting or on the radio by a terrorist organization, and section 4 defines “support of a terrorist organization” as including, inter alia, oral or written publications\(^{439}\) of sympathy or call for support of the terrorist organization; possession of propaganda material for such an organization; support with money or monetary equivalent; placing an object or place at the disposal of the terrorist organization. Here too, there is great lack of clarity: it is unclear whether these prohibitions apply only to the contents provider (the actual speaker), or also to the provider of the advertising platform. Notwithstanding, the courts interpreted the Ordinance in a restricted sense, in light of its direct infringement of basic rights, such as freedom of speech.\(^{440}\)

Another restriction of free speech exists in the Press Ordinance, which requires a license from the Minister of the Interior for publishing of a newspaper and gives the Minister the power to close a newspaper.\(^{441}\) It seems that in light of the infringement of freedom of speech, the law should not be interpreted on a broad basis. Accordingly the Ordinance does not apply to the Internet, and a license will not be required for setting up of an Internet site. There seems to be no disagreement with this position.

**D. Summary of Recommendations**

The first question that must be placed on the legislature’s agenda is evaluation of the need for particular legislation as regards service providers’ liability for harmful content of third parties. The question involves examination of the actual conduct of the service providers in the absence of regulation: Does uncertainty cause undesirable

---

\(^{439}\) The term publication for the purposes of the Ordinance is defined in the Penal Code Law 5737-1977, in Section 34 (24): “Publication – document, printed matter, computer material, or any other visual exhibit, and all audio means, liable to raise words or ideas, either alone or with the use of any means”.


\(^{441}\) The discussion in of the **Kol Ha’Am** case was based on this power. See HCJ 73/53 “**Kol Ha’Am**” **Ltd. V. the Minister of the Interior**, P.D 7, 871. Also in this matter, see HCJ 644/81 **Omer International Inc. v. the Minister of the Interior**, P.D 36(1), 227 (appeal against order for cessation of publication of respondent’s newspaper). The order was issued by virtue of the Press Ordinance after the newspaper published praise of terror acts).
results? It is necessary to examine whether the providers do not provide specific services (chat rooms, forums, site storage service etc.) or restrict expression in the different applications that they operate. It is necessary, for instance, to examine how a site storage service provider reacts to a complaint of surfers against another site, or against the words of another surfer in a forum operated by that provider.

- If it is found that the existing legal uncertainty leads to the existence of “private censorship” then the legal situation must, we feel, be clarified through legislation.

- Such legislation must minimize the undesirable impacts discussed above. In particular, it must be verified that the discretion exercised by the provider is defined as precisely as possible and leaves the provider a clear and limited area of decision. In this way we will minimize the “chilling effect”, the “itchy finger” of the provider to close sites and other applications, and the leaving of public discretion in private hands.

- In our opinion, each of the existing models reviewed above (full liability, full immunity or conditional and restricted immunity) has considerable disadvantages.

- We feel that an approach of uniform regulation for different types of harmful contents must be adopted: whether defamation, infringement of privacy, infringement of intellectual property rights or terrorist propaganda.\(^{442}\)

- The general principle established in the American legislation of immunity for intermediate agencies should be adopted, but it should be qualified with an exception: in order to protect the interests and rights, an effective enforcement channel must be allowed for injured parties, by action in court. In this way our proposal differs from American law. The court will be required to weigh the public interest or the right of the protected individual, against considerations of public and other policies and interests. In this way it will be

\(^{442}\) It should be noted in this context that the reason for the differential American approach is unclear. It derives apparently from economic and political pressures exercised by commercial lobbies. For a general discussion of the influence of lobbies on American legislation in the context of copyrights, see: Jessica Litman, *Digital Copyright* (2001).
guaranteed that the legislative, moral checks and balances developed in case law will be safeguarded, and will not be privatized in the commercial service provider. The court’s power will be limited to issuing of injunctions only.

- As long as a court has not ordered a provider to act, the service provider will enjoy immunity from damage claims.