The Haifa Center of Law and Technology Publication Series

Publication No. 7

Privacy in the Digital Environment

by

Students of the Interdisciplinary Law & Technology Workshop
Faculty of Law, University of Haifa

2005

Haifa Center of Law & Technology
Some rights reserved to the Haifa Center of Law and Technology, 2005.
This publication is licensed under a Creative Commons Attribution 1.0 Israel License.
Fair use of this position paper is welcome.

ISBN 965-90924-1-5

Please quote as follows:
Yael Onn et. al., Privacy in the Digital Environment (Haifa Center of Law & Technology, Niva Elkin-Koren, Michael Birnhack, eds., 2005).

The Haifa Center of Law & Technology

Haifa Center of Law & Technology (HCLT) is a research institute based at the Faculty of Law, University of Haifa. The main goal of the center is to promote research activities in the fields of Law and Technology and similar areas. HCLT conducts workshops and conferences, open to academics and to the public. HCLT encourages research on varied topics in the field of law and technology and intellectual property by faculty staff and by students. HCLT grants scholarships and hosts lectures by leading lecturers from Israel and other countries.

Haifa Center of Law & Technology, Faculty of Law, University of Haifa
Mount Carmel, Haifa 31905 Israel
Tel: +972-4-828-8569, e-mail: techlaw@law.haifa.ac.il,
website: http://techlaw.haifa.ac.il
The team of authors

Yael Onn       Michael Geva
Yaniv Druckman  Ariel Zyssman
Rom Timor      Inbal Lev
Arz Maroun     Tamar Maron
Yossi Nachmani Yaniv Simsolo
Saar Sicklai   Adi Fuches
Maor Fishman   Shai Packer
Lotem Pery

Supervisors and editors

Professor Niva Elkin-Koren       Dr. Michael Birnhack

In collaboration with
The Caesarea Edmund Benjamin digital environment Rothschild Foundation Institute for Interdisciplinary Applications of Computer Science
## Table of Contents

Executive Summary vii  
Foreword and Acknowledgements xiv  

1. Introduction 1  
   A. The Right to Privacy - The Theoretical Basis 1  
   A.1. The Right to Privacy - General 1  
   A.2. The Conceptual Difficulties in Defining the Right to Privacy 1  
   A.3. What is the Right to Privacy? 5  
   A.4. The Justifications for the Right to Privacy 12  
   A.5. The Interests Conflicting with the Right to Privacy 16  
   A.6. Interim Summary 19  
   
   B. Privacy on the Web 21  
   B.1. The Digital Environment and the Information Revolution 21  
   B.2. Awareness, Anonymity, the Ease of Use and the Absence of Boundaries 23  
   B.3. A Renewed Ethical Examination of the Appropriate Balance between the Different Values in the Digital Environment 29  
   B.4. Interim Summary 33  
   B.5. Protection of Privacy in the Digital Environment - Should It Be Regulated and How? 33  
   B.6. Interim Summary 44  

2. Digital Means of Surveillance 63  
   A. Introduction 63  
   B. An Examination of the Various Aspects of Digital Means of Surveillance 64  
   C. Possible Solutions 99
Executive Summary

1. **Introduction**
   
   **A. The Right to Privacy: A Theoretical Basis**

   1. It is difficult to define the right to privacy, since privacy is not a pure legal term - it has psychological, social and political aspects. The conceptual difficulties in defining the right to privacy are due to the fact that various interests protected by the right are also protected by other laws and due to the fact that privacy is affected by political, social and economic changes and by technological developments.

   2. After reviewing the various definitions of the right to privacy in the case law and in academic literature, it is possible to formulate a definition which includes elements of both access and control:

   The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, thoughts, feelings, secrets and identity. The right to privacy enables us to choose which parts in this domain can be accessed by others, and control the extent, manner and timing of the use of those parts we choose to disclose.

   3. It is important to note the theoretical justifications of the right to privacy, so we can face technological, social and other changes and to draw the borderline between the violations we wish to prevent and those we can allow. One type of justifications views the right to privacy as an end in itself: these justifications view the right to privacy as a means for realizing human autonomy; for keeping one's peace of mind; for encouraging freedom of speech, which can be violated if one knows he or she is being watched or that her or his conversations are tapped, and for protecting the freedom of research: the ability to search, read and receive information without fear. Another type of justifications sees the right to privacy as a means for achieving other interests: equality and narrowing the social divide; encouraging companionship, love and trust in people's relationships; allowing for the accumulation of power, leading to leadership; the ideal of the rule of the people, democracy and free society.
4. There are many substantial justifications for the right to privacy, yet there are certain violations of privacy that we are willing to suffer, in order to maintain a proper balance between the right to privacy and conflicting interests. Like all other fundamental rights, privacy is not an absolute right. Such interests may include freedom of speech and the public's right to know, law enforcement or economic interests.

B. Privacy in the Digital Environment

5. In the context of privacy, the technological developments have created a new reality, on both the legal and the practical level. While technological progress has changed the rules of the game completely, the legal system lags behind. While lawyers are still thinking over the appropriate form of regulation and its appropriate boundaries, the violators of privacy are accumulating knowledge, power and information and impose norms of conduct which will be almost impossible to uproot. A reality where there is no law and order raises the question: is it still possible to protect privacy? All of these issues lead to legal questions about the appropriate scope of the right to privacy and the choice of the best form of regulation.

6. The options for handling the threats to privacy are public regulation (direct or indirect) and/or private regulation.

Direct public regulation (legislation determining directly what is allowed and what is prohibited) can be achieved through implementing the general law of the physical world to the digital environment, or through the making of new legal rules. Its advantages are transparency, legal certainty and granting a moral approval to the protection of privacy. Its disadvantages are compromising the decentralized public discourse typical to the digital environment, an attempt to subject technology to the legal rules, which in many cases is bound to fail, and inefficiency on a global level.

Indirect public regulation (legislation creating incentives, either positive or negative, but does not determine directly what is prohibited) gives legal incentives to private regulation. Such regulation does indeed resolve most of the disadvantages of public regulation, but creates difficulties due to privatizing public discretion (see below).
**Private regulation** is achieved by market forces through technological solutions, privacy policies and contractual arrangements, by ethical codes, education and diffusion of social norms. Private regulation maintains the freedom typical of the digital environment, but is problematic since it privatizes public discretion, delegating it to private bodies with interests that are not transparent.

With regard to any threat presented in this position paper we shall ask **whether it appropriate** to intervene and regulate this phenomenon? If we reach the conclusion that it is, we shall try to examine the appropriate **means** of interventions and its appropriate **extent**.

C. Consent

7. Consent is at the core of the right to privacy. With one's consent, the action concerned does not constitute a "violation of privacy." The Israeli law defines consent as both explicit and implicit. Is this element compatible with the digital environment?

8. Our conclusion is that the attempt to rely only on the existing law has failed. In practice the law is incompatible with the new reality, and in any case it is not implemented and not enforced. The model we have focused on is giving information and creating unity. We borrow the "informed consent" model used in medical law. Despite the substantial difference between bodily harm and violation of privacy, some interests worthy of protection are common to both areas. Among these is the wish for free choice and autonomy, long recognized as basic rights. Beyond the protection of these interests, it should be acknowledged and understood that the situation as it exists today is problematic and allows for violations. The same considerations that led the legal system to intervene with the relationship between a physician and his patients should justify its intervention with the relationship between users and web site operators.

9. The existing legislation regulated consent in the legal world, but it is insufficient and is incompatible with technological developments. New solutions must be found for the new situation created and for the many difficulties of enforcing the legal framework in a virtual environment. A partial solution, in the absence of a better
alternative, can also improve the legal situation. The fear of the unique problems of the digital environment is real, but this does not justify standing still and creating a lacuna that enables the violation of privacy, which is a basic right under Israeli law.

10. One possible solution, also suggested in the bill drafted by the Ministry of Justice, now part of a bill submitted to the Knesset, is determining a level of "informed consent" with regard to certain types of information.

2. Digital Means of Surveillance

11. There are various means of surveillance in the digital environment. They can be classified as follows:

a. One group includes means of surveillance aimed mostly at monitoring the activity of the end users, and have no other use which is not negligible compared to the harm they cause (spyware, Trojan horses, Internet bugs and various spyware programs that can be easily obtained on the web). With regard to these, legislative amendments should be made (public regulation), to impose on the spying party a duty of disclosure, which should be clear and targeted at the reasonable user, and to receive the user's full prior consent. On this issue we support the Ministry of Justice bill, which suggests a level of "informed consent" imposed on the web. In the absence of such consent, the hostile action should be seen as a violation of privacy.

b. Another group includes means that have other uses, not having peripheral significance compared to the damage they cause (cookies, sniffers and cellular phones). These are means of surveillance but surveillance is not their main purpose and the violation of privacy that they cause is only incidental. In general terms, with regard to this group of means of surveillance, private regulation solutions are called for, including a code of ethics, recruiting the market forces and using technological solutions and standards that are different to those of commercial bodies or non profit organizations. In addition, legislation is another possible solution, to ensure that the borderline between the beneficial use - usually forming an integral part of the technology - and the use causing a violation of privacy is maintained. For example, legislation to endure that the cellular phone companies do not use the geographical information created during use of a cellular phone for marketing purposes, unless the user gives her express consent to such use. To a certain extent, this is the legal
situation today, based on section 2(9) of the Privacy Protection Act of 1981 (PPA) and the requirement of consent in section 1 of the Act.

3. **Databases**

12. Databases raise many difficulties. Chapter B of the PPA attempts to address some of them. Indeed, there is a need for **special legislation** with regard to computer databases. However, there is a need to increase awareness and to educate the public on responsible conduct in society in general, about the risks involved in using the web and particularly about disclosing information.

13. The European and Israeli approach, supporting direct public regulation of privacy in general, and of databases in particular, is essentially correct. **A central privacy protection institution is called for**, preferably a public non-governmental authority, and in any case, an independent authority.

14. It is doubtful whether the existing arrangement under the Privacy Protection Act, whereby a duty of registration is imposed, can still stand.

15. The powers of the supervising institution should be wide enough in order to enable effective and active enforcement. The powers should include imposing specific conditions and limitations on certain types of databases, on databases in a particular area of occupation or field of industry, limitations on specific database owners and on specific databases. The supervisor should have the power to impose administrative sanctions, such as fines, closing down businesses and imposing personal liability on managers (subject to a just procedure and the rules of administrative law, of course). The supervising body should be allowed, for the purpose of supervision, to inspect and examine the databases and to receive complete information on their management. The option of allowing the supervising institution full access to the databases should be considered, where there is reasonable suspicion and other guarantees, in order to prevent abuse of power.

16. Submission of a complaint to the supervising body should be as free as possible, without fees. The Internet should be used as a low cost, efficient tool for serving the citizens.
17. Citizens should be allowed access to the data on the databases, and this should be as free as possible, considering the sensitivity of the information. Clients should be informed of the information about them being accumulated and of their rights with regard to such information, in a complete, convenient and low cost manner. For example, when the information is already available on the Internet for the use of employees, it should also be disclosed to the relevant clients. Where databases are disclosed on the Internet, substantial weight should be given to the interests and rights of the database owners and their business conduct.

18. In addition, **private regulation and self regulation of privacy protection in running databases should be encouraged**. The use of torts law can be effective in regulating privacy protection. Incentives should be created in order to encourage self regulation, its maintenance and self enforcement.

19. A body holding *public* information should be recognized as a *quasi*-public body. Such a body is subject to duties and norms of conduct and management derived from administrative law, or at least the parts of administrative law imposed on quasi public bodies under Israeli law. Examples include the duty of transparency, the Freedom of Information Act, the duty to give reasons for decisions, and exercise of discretion in a reasonable and proportionate way by the database operator, all of which combined will create a greater degree of fairness in the database environment.

20. With regard to a private body not holding public information, but holding a large amount of information or particularly sensitive information, we ought to consider imposing similar duties when the information it holds is essentially similar to public information.

21. Any regulation of computer databases depends on **stable, comprehensive and well-defined legislation in the general field of computer crime**.

4. **Privacy at the Workplace**

22. In order to provide effective protection of the privacy of employees, public regulation (direct or indirect) is required. **Direct regulation** should be similar, in our
opinion, to the European approach, which focuses on informing the employee. The advantages of this approach are the technological neutrality and examining the employee's expectations compared to the extent of the violation of his privacy.

23. A possible solution for the problem of the employee's consent to the violation of his privacy is examining the employer's activity under the administrative law tests of a proper purpose, proportionate means and the absence of an effective alternative. In addition, a "routine" situation should be distinguished from an "unusual" situation at the workplace and monitoring contents should be distinguished from monitoring activity.

24. Direct regulation can also be achieved by creating incentives for class actions on violation of employees' privacy.

25. Under collective labor law, the trade union should be able to bring action against the employer for violation of employees' privacy. In addition, we consider establishing joint committees of the employer and the trade union under legislation, to discuss the disputes relating to violation of employees' privacy.

26. Combined with the direct regulation, we should also consider indirect regulation, giving incentives to employers to protect the employees' privacy (for example, partial exemption from vicarious liability when use is made of technological tools owned by the employer). Additionally, indirect regulation can be part of existing collective agreements.
Foreword and Acknowledgments

The digital environment enables new uses of information: in the ways it is collected, processed, saved and distributed. These technological changes create, on the one hand, new business opportunities, and on the other hand, new threats to privacy. Privacy is seen as a basic right, constituting an essential element in creating a safe environment for electronic trade and at the same time is used to disguise criminal and terrorist activities, and therefore is of interest to the law enforcement authorities.

The Haifa Law and Technology Workshop held in 2004 focused on the question of privacy on the web in general and in particular in Israel. We tried to understand the needs of the industry, the players in the electronic trade arena, the state and the law enforcement authorities and, of course, users. We examined various technological possibilities of surveillance, gathering, processing and using information. The technological possibilities were placed in the framework of Israeli law, relying also on comparative law, and we raised the question of whether the law should intervene, and if it should - in what way and in which cases, and what are the alternative solutions that the market and technology offer. The workshop participants were fifteen carefully selected students of the Law Faculty at the University of Haifa.

The Law and Technology Workshop is a unique research institute dealing with practical questions in the field of information policy. Policy design in the area of law and technology takes place not only in the courts, but also - and to a large extent - in the Knesset and the various state authorities. Policy designers who need information, data, evaluations, analysis of the meaning and implications of the policy, so they can determine their course of conduct, are fed mostly by interest groups that provide data promoting their own interests. The public voice is hardly heard at these discussions. In addition, many companies, especially new start-up companies, need legal guidance on issues of public concern. The aim of the Law and Technology Workshop is to fill this gap.

The research and writing at the workshop were conducted in several stages. After an initial brainstorming and deciding on the research topics, the participants were divided into work teams by topic. The research process continued with face-to-face meetings
and group discussions through an Internet forum, in which questions and issues were clarified. After the research and the first draft of the position paper were completed, we considered that there was room for learning the positions of experts and professionals in the fields we dealt with. This is how the Neve Ilan Conference came into being (December, 17-19, 2003). We discussed the relevant issues for three days with dozens of experts from different fields of research and occupation, in particular computer science and law. The lawyers were academics, private market lawyers and public service lawyers. The dynamics created during the three day conference, the lectures and the fruitful discussions emphasized the need for impartial discourse and independent multi-disciplinary research on subjects relating to law and technology.

During the editing of this position paper, the Ministry of Justice published a Bill for the Privacy Protection Act (Amendment - Privacy of the Deceased, Informed Consent and Compensation without Proof of Damage), 2004. During the English translation, the Bill was submitted to the Knesset, with some modifications, and at the time of writing is pending. The bill does not suggest a comprehensive reform in the protection of privacy law, but has some suggestions for important amendments relating to the issue of privacy protection in the digital environment. These days, a committee chaired by the deputy of the Attorney General, Yehoshua Shuffman, is examining the regulation of databases. We hope that this position paper can benefit the public discussion. The position paper was produced by the work of the students at the workshop and represents their collective position, and it does not necessarily reflect the position of their current workplace or of the editors.

The lessons of the research and of the Neve Ilan Conference are summarized in this position paper. On many issues, the position paper represents a first attempt at dealing with questions that have not yet been the subject of public discussion in Israel. We hope that this position paper will be the basis of a serious discussion on questions that require definitive answers and will assist in designing informed policy.

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 (CRI). 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. We would also like to thank Ms. **Libby Oded**, the Institute’s administrative coordinator at the time. We would like to thank the members of staff at the Faculty of Law at the University of Haifa, who assisted us: the previous Dean, Professor **Ariel Bendor**, the current Dean Professor **Eli Salzberger** and **Yotam Vered**, then the faculty's Computing Coordinator.

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 alphabetical order):

**Shlomi Onger**, "Mahshava" CEO; **Dan Or-Hoff**, Adv., Ravia & Co. Advocates; Dr. Yuval Elovici, Information System Engineering Department, Ben Gurion University of the Negev; Slav Ben-Ari, Adv., tmicha.net; Professor **Ariel Bendor**, Dean of the Faculty of Law, University of Haifa; Dr. **Yossi Berg**, Legal Advisor of the Israeli Consumer Commission; **Amir Gans**, Business Manager, New Approach; **Rivki Dvash**, Adv., Consultancy and Enforcement Department, Ministry of Justice; **Yossefa Tapeiro**, Adv., Database Registrar, Ministry of Justice; Dr. **Guy Davidov**, Faculty of Law, University of Haifa; Dr. **Moshe Cohen-Elia**, the Academic College of Law, Ramat Gan; Dr. **Naama Carmi**, University of Haifa and the Interdisciplinary Center, Herzliya; **Amir Lev**, President of Commtouch; **Alon Mollian**, Vice CEO, MRM; **Haim Klugman**, Adv., Chair of the Public Commission for Protection of Privacy; Judge **Gabriel Kling**, former Vice President of the Tel Aviv District Court; Dr. **Yuval Karniel**, School of Law and School of Media Studies, the College of Management; Dr. **Rivka Ribak**, Media Department, University of Haifa; **Yehoshua Shoffman**, Adv., deputy to the Attorney General; **Amir Shor**, Client Solutions, Barak 013; **Eyal Shief**, Privacy Officer at Dotomi; Dr. **Bracha Shapira**, Information System Engineering Department, Ben Gurion University of the Negev.

We also wish to thank other participants who contributed to our Workshop: Adv. **Eran Bareket**, Adv. **Gil Granot-Meir**, Adv. **Dalit Dror**, **Ronen Housirer**, Elad
Wieder, Dr. Amir Khuri, Nahman Liss, Professor Motti Meroni, Ran Kamil, Adv. Haim Ravia, Orli Reichman, and Ariel Schwartz.

The production of the conference could not have taken place without the dedicated work of Inbal Lev, the former coordinator of the Haifa Center of Law and Technology, and this paper was produced thanks to the dedicated work of Elad Wieder, current coordinator of the HCLT.

Niva Elkin-Koren, Michael Birnhack

Haifa, March 2006
1. **Introduction**

A. **The Right to Privacy - The Theoretical Basis**

A.1. The Conceptual Difficulties in Defining the Right to Privacy

This chapter seeks to establish the theoretical basis and guidelines for the discussion on the specific issue of privacy in the digital environment. The chapter consists of three sub-sections. First, we shall examine the theoretical basis of the right to privacy, the conceptual difficulties involved and the attempts to define the right, and suggest a "working definition." We shall examine the main justifications of the right to privacy and the relevant conflicting interests. We shall examine the main characteristics of the digital environment related to the right to privacy. We do not attempt to provide a comprehensive examination of the digital environment, but only an instrumental examination for the purpose of the discussion on the right to privacy. The chapter will conclude with a thorough examination of the concept of consent in the context of privacy. In our opinion, this is an important concept in the discussion on the question of privacy in general and in particular in the context of the digital environment.

A.2. The Conceptual Difficulties in Defining the Right to Privacy

What is the right to privacy that we seek to protect? This is not a simple question, and it has many answers. A lot has been written on the subject, since privacy is not only a legal concept: it has psychological, social, cultural and political aspects. However, even limiting ourselves to defining the legal aspect of privacy, is a difficult task. It appears that the conceptual difficulty in finding an accepted legal definition of the right to privacy is caused by its characteristics. In order to define the right to privacy for the purpose of this position paper, we shall begin with examining those characteristics of the right to privacy which render it hard to define.

---

1 This chapter is based on lectures by Dr. Michael Birnhack in the course "The Right to Privacy" (University of Haifa, 2004) and "Information Law in the Digital Environment" (University of Haifa, 2003) and on lectures by Adv. Dan Or-Hof and Adv. Haim Ravia in the course "Evidence, Offences and Computer Torts" (University of Haifa, 2003), as well as on the things said by participants in the "Privacy on the Web" Conference that took place in Neve Ilan on December 17-19, 2003 (hereinafter: the Neve Ilan Conference).

2 In the Report of the Cohen Committee, following which the PPA was enacted, it was maintained that Privacy is one of the legal terms that has no accurate definition. See Report of the Committee on Protection of Privacy, in the *Yitzhak Cohen Book* (M. Elon, M. Ben-Zeev, A. Barak, N. Lifshitz and M. Landoy eds., Tel Aviv, Papyrus, 1989), pp. 87, 88.

One such characteristic is the fact that various interests protected by the right to privacy are also protected by other laws. Thus, for example, the constitutional protection of human dignity in Israeli law relates also to invasion of privacy which violates one's dignity;\(^4\) criminal law grants protection from bodily harm\(^5\) or penetration without consent;\(^6\) property law protect the physical domain;\(^7\) tort law protects against trespassing,\(^8\) assault\(^9\) and violation of privacy which amounts to nuisance;\(^10\) the Prevention of Stalking Act of 2001 provides protection from stalking and threats;\(^11\) and the Anti-Defamation Law of 1979 prevents another from publishing misleading information that harms one's reputation;\(^12\) copyright law protects, \textit{inter alia}, unpublished works;\(^13\) the Wiretapping Act of 1979 ensures that communications are not tapped without the consent of the parties to the conversation or under strict judicial oversight;\(^14\) codes of ethics in various areas protect the secrecy of information disclosed to physicians\(^15\), psychologists\(^16\) and advocates,\(^17\) and many more examples.

Thus, we see that the interests protected by the right to privacy are similar to some extent to those protected by other rights. Therefore, some argue that the right to privacy should not be defined as a separate legal right.\(^18\) According to this approach, the protection granted by other laws to the various interests that constitute the right to

---


\(^6\) Section 345 of the Penal Act.

\(^7\) Sections 15-20 of the Property Act, 1960, Laws of the State of Israel 269.

\(^8\) Section 29-31 of the Torts Ordinance (New Version), Laws of the State of Israel 266 (hereinafter: the Tort Ordinance).

\(^9\) Section 23 of the Tort Ordinance.

\(^10\) Sections 42B-48 of the Tort Ordinance.

\(^11\) Prevention of Stalking Act.

\(^12\) Anti Defamation Act, 1956, Laws of the State of Israel 240.

\(^13\) Section 1 of the Copyright Act, 1911, Laws of Israel, Vol C., 2533.


\(^15\) Section 19 of the Patient's Rights Act, 1996, Laws of the State of Israel, 327.

\(^16\) Section 7 of the Psychologists' Act, 1977, Laws of the State of Israel 158.

\(^17\) Section 90 of the Bar Association Act, 1961, Laws of the State of Israel 178.

privacy - is sufficient.\textsuperscript{19} In this position paper, we argue that the right to privacy should be seen as an independent right that deserves legal protection in itself. Our opinion is based on several grounds.

Firstly, there are interests that can only be protected by the right to privacy. For example, defamation law does not protect a person's right not to have true personal information published. In addition, one can look into a person's house, into the physical domain, without invading it and violating one's property rights, or take pictures of a person without permission in the public domain where the person has no property rights. Indeed, it may be argued that the inclusion of the right to privacy as part of the constitutional right to human dignity can serve as a general protection for the types of violations that are not covered by other laws, but this argument fails for two reasons. First, the Basic Law: Human Dignity and Liberty is addressed primarily at the authorities, rather than individuals and private bodies.\textsuperscript{20} Moreover, it has been maintained in the case law that violation of any right shall be considered as violation of dignity only if it amounts to humiliation.\textsuperscript{21} Therefore, there are violations of the right to privacy that cannot be defined as a violation of dignity. For instance, it appears that collecting one's identifying details - name, address or identity number - without misuse of these details, does not amount to violation of human dignity.

Secondly, if we do not protect the right to privacy as a separate independent right and rely only on the protection provided by other laws, there is a risk that it may be conceived as a marginal, unimportant right. By calling a series of interests "the right to privacy" we indicate that this right is a central one in the eyes of the law and grant it a moral approval. Moreover, there is an educational element in defining privacy as a right, in increasing public awareness to the importance of protecting privacy and deterring from privacy violations.

\textsuperscript{19} Ibid, at 286.

\textsuperscript{20} Section 11 of Basic Law: Human Dignity and Liberty provides as follows: "All governmental authorities are bound to respect the rights under this Basic Law." However, there is a theory that applies the constitutional rights to private law in some cases. See: Aharon Barak, \textit{Legal Interpretation - Constitutional Interpretation} (vol. 3) 441-446, 649-697; Aharon Barak "Human Rights Protected under Private Law" in \textit{Klinhofer Book of public Law} (Yitzhak Zamir, ed., 163); \textit{Hevre Kadisha v. Kastenbaum}, 46(2) P.D. 464, 530.

\textsuperscript{21} Per Justice Dalia Dorner in HCJ 4541/94 \textit{Miller v. Minister of Defense}, 49(4) P.D. 94, 132: "there is no doubt that the purpose of the Basic Law id to protect an individual from humiliation. Humiliation harms one's dignity. There s no reasonable way to interpret the right to dignity established in the Basic Law without considering humiliation as an infringement thereof. Indeed, not any inequality amounts to humiliation; therefore not any inequality infringes the right to dignity."
Third, if we divide the right to privacy into components, each protected by a different law, it will be hard to create appropriate rules for privacy protection that can apply to any type of violation. At the basis of every law lie conflicting interests forming part of the structure of the legal rule and expressed in every aspect thereof. These interests do not necessarily serve the right to privacy. Indeed, should we unify all interests protected by the right to privacy we may lose some of the protections granted to the right to privacy by other laws, but the legal regime we create shall represent an appropriate balance between privacy and other conflicting interests.

So far we have discussed one difficulty in defining the right to privacy - the certain overlap between the interests protected by the right to privacy and the interests protected by other laws. Another characteristic of the right to privacy which contributes to the difficulty in defining it is the fact the right to privacy is subjective in nature, culturally dependant, and is derived from the expectations of the society in a certain period of time. Therefore, privacy has been given different meanings over the years, being influenced by political, social and economic changes and by technological developments.

Some consider the right to privacy a natural tight - an ancient principle. Others argue that the right to privacy is a context-dependant legal right, born as a result of the needs of society and designed in accordance with changes in society and in technology that developed the awareness of its importance and the public and legal discourse about it. It appears that the truth lies between these two approaches. Indeed, privacy, as a social norm, has long been common. In all societies in all periods in history, the importance of privacy was recognized, for the individual, the intimate family unit and the whole community. Research shows that privacy is not only a human need, but other animals need also need time for themselves or intimacy in

---

22 Dr. Naama Carmi, lecture at the Neve Ilan conference, 17 December 2003.
23 Dr. Rivki Ribak, lecture at the Neve Ilan conference, 18 December 2003
24 Samuel Warren & Louis Brandeis, "The Right of Privacy", 4 Harv. L. Rev.193 (1890)
small groups.\textsuperscript{26}

However, even if privacy is a natural right, there is no doubt that its value has grown over the years and its realm has been extended.\textsuperscript{27} Real life dynamics have frequently presented to society challenges, needs and situations that required rethinking about the balance between the right to privacy and conflicting values.\textsuperscript{28} The elements that contributed to this reality included social and cultural developments, such as the formation of a household consisting of the nuclear family, the autonomy of urban living and the mobility with regard to places of residence and work;\textsuperscript{29} the rise of democracy, which increased the need for privacy, as society becomes more open and has a greater tendency to intervene with its citizens' affairs, whether through the authorities or the media relying on the principle of the public's right to know;\textsuperscript{30} and the new technological opportunities/threats to the right to privacy, which increased the possibilities for violation of privacy and the extent of such violations - the tabloid press, photography, radio, television and cellular communications and of course, the Internet.\textsuperscript{31}

In light of all these factors, it is no wonder that the conceptual question about the right to privacy appears again and again on the public agenda. As society changes, as the possibilities for violations increase, it becomes more difficult to define the legal right of privacy. Therefore, we seek to formulate a flexible definition of the right to privacy, which can predict the future, as far as possible.

A.3 What is the Right to Privacy?
Thus far we have examined the difficulties in defining the right to privacy. We shall


\textsuperscript{27} In ancient societies only specific situations were regarded as private, such as nudity, intercourse, birth, illness or death. (Westin, supra note 25, at 62). Nowadays the right to privacy is much broader.

\textsuperscript{28} Levin, \textit{supra} note 25, at 173.

\textsuperscript{29} \textit{Ibid}, at 69.

\textsuperscript{30} HCJ 2481/93, Dayan v, Vilk, 48(2) P.D. 456, 487.

\textsuperscript{31} In the words of Minister of Justice Shmuel Tamir presented to the Knesset the proposal of the Privacy Protection Act (PPA): "In a democratic country the need to protect one's right to privacy is recognized... the essence of this need is not permanent and may change with time... what was taken for granted decades ago has changed hen the ways to violate privacy have become more sophisticated, when it is possible to see and hear from an enormous distance not only what one does or says, but even his heartbeats, blood pressure and body temperature."
now attempt to overcome those difficulties and try to find a definition that includes all the interests we consider worthy of protection nowadays under the term "privacy."

In general, the term "privacy" can be defined in two ways. One way is to create a legal rule describing various circumstances involving the individual and other people that should be considered privacy violations. A second way is to present an open, general definition, that will clarify the term. *Since the right to privacy is largely context-dependant, we consider that it should be defined as a standard, rather than a rule, by an abstract rather than a concrete definition. The definition should be abstract and wide, in order for it to be flexible enough to include additional interests that may be violated as a result of future developments.*

A legal rule describing the situations that should be considered as privacy violations protects our reasonable expectations, but these expectations change, as aforesaid, with time and technological developments. Even where such a rule seeks to shape our expectations and include new types of privacy violations beyond our reasonable expectations, presumably the rapid technological developments will soon catch up with the legal definitions. In this sub-chapter we examine the various definitions of the right to privacy over the years in the legislation, the case law and the legal literature in Israel and elsewhere, while trying to formulate our own definition.

Under Israeli law privacy is protected both by section 7 of Basic Law: Human Dignity and Liberty, rendering it a constitutional right, and by the PPA. The Basic Law: Human Dignity and Liberty does not define the right to privacy, but stipulates in section 7(a) that "every person has the right to privacy" and elaborates on the elements of the right which are granted constitutional protection:

"(b) There shall be no entry into the private premises of a person who has not consented thereto."

(c) No search shall be conducted on the private premises of a person, nor in the body or personal effects

(d) There shall be no violation of the confidentiality of conversation, or of the

---

32 Adv. Tana Shpanitz, Deputy Attorney General, is of the opinion that some areas that are influenced by technological developments had better be regulated through legislation with general principles, accompanied by specific regulations that can be amended more easily (Law & Technology Workshop, Neve Ilan, 11 December 2002).


34 Laws of the State of Israel 128.
writings or records of a person."

The PPA does not define the right to privacy, but sets out in section 2 a closed list of specific interests that form a violation of privacy and are protected under the Act. Judge Gabriel Kling, who took part in the legislation process of the PPA, says that this list was created since the Act was enacted at a time when the right to privacy was not an established legal right and the public was not aware of it. The closed list of various situations describing privacy violations leads to recurring lacunas in the PPA and creates a lack of clarity as to the extent of the right to privacy.

In the Israeli case law, there is no uniform definition of the right to privacy and its extent is unclear. The Supreme Court recognized that the definition of the constitutional right to privacy is influenced by human experience and must adapt itself

35 Section 2 of the PPA provides that violation of privacy is any of the following:
(1) Spying or following a person in a manner that may cause harassment;
(2) Unlawful monitoring;
(3) Photographing a person in his private domain;
(4) Publishing a person's photo in public in circumstances that may humiliate him;
(5) Copying the contents of a letter or other document not intended to be published, or use of its contents without the permission of the recipient or author, unless it is of historical value
(6) Use of a person's name, photo or voice for profit;
(7) Breach of the duty of secrecy about a person's private matters under law;
(8) Breach of the duty of secrecy about a person's private matters under an express or implied contract;
(9) Use of information one a person's private matters or giving it to a third party for a purpose different from that for which it was originally given;
(10) Publishing something obtained through a violation of privacy under ss.(1)-(7) and (9) above.
(11) Publishing something relating to a person's intimate life, health condition or conduct in his public domain.

36 Judge Gabriel Kling, Workshop, lecture at the Neve Ilan workshop, 18 December 2002.
37 Adv. Haim Klugmann, Chair of the Privacy Protection Commission, lecture at the Neve Ilan workshop,, 18 December 2003.
38 In some cases the definition of the right to privacy was excessively narrow. For example where a detainee was forced to drink salty water in order to make him vomit drugs, the police's action was not regarded as a violation of privacy, although seemingly there is no dispute that it includes' one's body (DN Vaknin, supra note 25). The majority interpreted the PPA narrowly, assuming that it was intended to create new boundaries (supra, at 851). Therefore it was held that there was a violation of privacy but it was marginal compared to the harm to bodily integrity protected under other laws (supra, at 856). Only the minority opinion of Justice Bach used a test based on common sense and life experience and recognized the violation of privacy (ibid, at 863).
39 Dayan, supra note 30, at 470.
8 | Privacy in the Digital Environment

to the changing reality. In some cases, the right to privacy was given a wide definition. For example, President of the Supreme Court, Aharon Barak, defined the right to privacy as follows: "The right to privacy draws a borderline between the individual and the public, between "me" and society; it draws a realm in which one is left to on his own, with no intervention from others." A wide definition was also set by Justice Tova Strassberg-Cohen, who adopted the definition offered by Professor Zeev Segal, according to which the right to privacy embodies "the right of the individual not to be disturbed in the privacy of his life by others".

Save for these few cases, the case law has chosen not to define the right to privacy, but to determine on a case by case basis whether the interest at hand is part of the right to privacy. In this manner, many diverse interests have been included in the definition of the right to privacy; therefore it is difficult to extract clear conclusions by reviewing the case law. Thus, for example, the interests recognized as part of the right to privacy include ones' right to run the lifestyle of his or her choice in his or her own home, without outside intervention; one's right not to have his or her body penetrated by a surgery or another forced action; parents' autonomy to make decisions about their children, without state intervention; one's right to have control of his or her life and to plan it, without intervention with his or her intimate decisions; the rights of an adopted child and his or her adopting parents to keep the adoption secret; information on one's mental health and many other examples.

Under US law, the right to privacy is protected by the constitution to a very restricted extent. The Fourth Amendment of the U.S. Constitution protects a certain aspect of the right to privacy, by stipulating that: "The right of the people to be secure

40 Ibid, ibid.
41 Ibid, at 471.
43 Dayan, supra note 30, at 470.
44 CA 506/88 Sheffer v. State of Israel, 48(1) P.D. 87, 188.
45 CA 226693 Anonymous, Minor v. Anonymous, 49(1) P.D. 221, 235.
46 DNA 2401/95 Nahmani v Hahmani, 50(4) P.D. 661, 682.
49 CA 7528/95 Hillel v. State of Israel, 50(3) P.D.89, 96.
in their persons houses, position papers and effects, against unreasonable searched
and seizures, shall not be violated…"50 Different aspects of the right to privacy are
protected in the US through specific laws.51

In 1960 Dean William Prosser examined all US cases in which the word
"privacy" was mentioned up until then and found it was used for four different
purposes: scclusion; publication of true yet private information; false light and
appropriation of a person's name or image for profit.52 Dean Prosser tried to find a
common ground between these interests, but concluded that the connection between
them was loose.53

Section 653A of the Restatement (Second) on Torts reflects Dean Prosser's
conclusions to a large extent. This section details the various violations of privacy to
be protected on the public level, but, like the Israeli PPA, does not define the right.54
Only some of the States adopted section 652A, as the provisions of the Restatement
are not binding and only constitute a recommendation for the desired state
legislation.

In newer constitutions in the world, the right to privacy is expressly
established.55 In addition, many international human rights documents from the 20th

50 The Canadian Constitution only protects a narrow aspect of privacy: "Everyone has the right to be
secure against unreasonable search or seizure" (The Constitution Act, 1982, Part 1 - Canadian Charter
of Rights and Freedoms, article 8).

51 See, e.g.: Electronic Communications Privacy Act, 18 U.S.C. §§2510-2521; Children’s Online
Privacy Protection Act, 15 U.S.C. §6501-6506. See also the chapter on databases below.

52 William L. Prosser "Privacy (A Legal Analysis)", in Philosophical Dimensions of Privacy: An

53 Ibid, at 124.

54 Privacy violations protected under section 652A of the Restatement (Second) on Torts are: i) the
unreasonable intrusion upon the seclusion of another; (ii) the appropriation of another’s name or
likeness; (iii) the unreasonable publicity given to another’s private life; and (iv) publicity that
unreasonably places another in a false light before the public

55 For example, section 2 of chapter 3 in the Swedish Constitution provides as follows:

(1) No record about a citizen in a public register may be based without his consent solely on his
political opinions.

(2) Citizens shall be protected to the extent determined in detail by law against any infringement of
their personal integrity resulting from the registration of information about them by means of electronic
data processing. Section 6 of chapter 2 provides as follows:

All citizens shall be protected in their relations with the public administration against any physical
violation also in cases other than those referred to in Articles 4 and 5. Citizens shall likewise be
protected against physical search, house searches or other similar encroachments and against
examination of mail or other confidential correspondence and against eavesdropping, telephonetapping
or recording of other confidential communications.
century include the right to privacy among the main human rights. In these documents there are similar provisions establishing the right to privacy as a right deserving legal protection, but they do not elaborate on the elements of this right that should be granted protection.\(^\text{56}\)

Much has been written on the right to privacy. We have chosen to present here several definitions that we can learn from and be inspired by when we attempt to define the right to privacy for the purpose of this position paper.

Some define the right to privacy as a right to prevent *access* to a person's

---

Section 10 of the German Constitution provides as follows:

**Privacy of letters, posts, and telecommunications** (amended 24 June 1968)

(1) Privacy of letters, posts, and telecommunications shall be inviolable.

(2) Restrictions may only be ordered pursuant to a statute. Where a restriction serves to protect the free democratic basic order or the existence or security of the Federation, the statute may stipulate that the person affected shall not be informed of such restriction and that recourse to the courts shall be replaced by a review of the case by bodies and auxiliary bodies appointed by Parliament.

Section 13 of the Swiss Constitution provides as follows:

**Protection of Privacy**

(1) Every person has the right to receive respect for his or her private and family life, home, and secrecy of mail and telecommunication.

(2) Every person has the right to be protected against abuse of personal data.

Section 12 of the Universal Declaration on Human Rights of 1948:

No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honor and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Section 8 of the European Convention on Human Rights of 1950:

1. Everyone 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 is 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, or for the protection of the rights and freedoms of others."

Section 17 of the UN Convention on Civil and Political Rights of 1966:

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. Everyone has the right to the protection of the law against such interference or attacks.

Section 7 of the European Charter on Basic Human Rights of 2000:

Everyone has the right to respect for his or her private and family life, home and communications.
private domain without his consent. See, for example, the famous definition by Samuel Warren and Louis Brandeis in their famous article of 1890: "the right to be let alone." In many senses this article gave birth to the legal concept of the right. Professor Ruth Gavison also suggests a definition, according to which the element which underlies our interest in privacy is the issue of access, whether by physical invasion into one's space, by purchasing private information about him or her or by removing his anonymity. Another definition which can be expressed in terms of access is suggested by Professor Zeev Segal, who asserts that the right to privacy embodies one's interest not to be disturbed by others in his private life, to protect the "self" from being invaded by society. This right includes one's freedom to decide what information about him or her should be kept hidden from the public. Other authors who dealt with the right to privacy add an element of control of the use of the information we choose to disclose to the public. This position is described in length by Professor R.G. Frey, who considers that the control of the sphere around a person is a key element in defining privacy. Similar approaches are those of Professor Charles Fried, who defines the right to privacy as one's control of the information that pertains to him or her both the amount of information he or she chooses to disclose and its quality, the approach of James Rachels, who adds that privacy also means control of the timing of disclosure and to whom it may be disclosed, and the approach of Professor Helen Nissenbaum, who maintains that the right to privacy includes the right to control the context in which the information is used, as it may be

57 This definition views the right to privacy as a liberty, rather than a claim. See David H. Flaherty, "On the Utility of Constitutional Rights to Privacy and Data Protection", 41 Case W. Res. (1991), 831
58 Warren & Brandeis, supra note 24.
59 Ruth Gavison, "The Right to Privacy and dignity" in human Rights in Israel - An Essay Collection in Memory of Hamman Shelah (Association for Civil Rights in Israel), 61,68.
60 Segal, supra note 42.
61 Ibid, at 178.
62 Ibid, Ibid.
63 On the distinction between "access" and "control" see Fighting Terror Online (Haifa Center of Law and Technology, 2002), available at http://techlaw.haifa.ac.il/papers/terror_info_eng.pdf: (hereinafter: Fighting Terror Online).
66 James Rachels, "Why Privacy is Important", 4 Philosophy & Public Affairs (1975) 323, 328.
taken out of context.\textsuperscript{67} Professor July Innes adds another aspect to the element of control - one's control of his \textit{intimate decisions}.\textsuperscript{68}

If we draw together all of these definitions into one comprehensive definition, including both the element of access and the element of control, we can state as follows:

\begin{quote}
The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as our body, home, thoughts, feelings, secrets and identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and to control the extent, manner and timing of the use of those parts we choose to disclose.
\end{quote}

A.4 The Philosophical Justifications of the Right to Privacy

We have noted that right to privacy changes with time as a result of social and technological developments, enabling the invasion of one's privacy by new means. To better handle these changes, and define the contours of the right, we need to explore the underlying theoretical justifications of privacy. The more solid theoretical perception we have, the more answers we shall have to questions raised in this position paper.

The various justifications of the right to privacy can be divided into two classes. One class includes those justifications that see the \textit{right to privacy as an end in itself}, i.e., as a liberal right reflecting human freedom,\textsuperscript{69} and the right to human dignity.\textsuperscript{70} These justifications explain the right to privacy as a means of protecting the \textit{autonomy} of human beings, being a tool for human development, for building one's individual identity, for self realization, creativity and learning.\textsuperscript{71} The right to privacy enables us to create an island around us; a physical or virtual space where we can

\begin{footnotes}
69 Alan Westin notes that privacy in modern society in which the state has substantial control over individual lives, has become a liberty rather than a need. (Westin, \textit{supra} note 25, at 70).
\end{footnotes}
deliberate, experiment and make mistakes, away from the public eye, without social pressure and without taking responsibility for our actions.\textsuperscript{72} Without a private space, that lets us be ourselves, formulate independent views and decide what is good and what is bad for use, we cannot truly be autonomous people.\textsuperscript{73} In the words of Robert Maclver: "Everything that grows first of all does so in the darkness before it sends its shoots out into the light."\textsuperscript{74}

The right to privacy also enables us \textit{peace of mind}. Living in a society involves many causes of stress and endless confrontations. The right to privacy is essential in order to keep one's physical and mental health, by creating a space where he or she do not have to confront others, act in accordance with accepted norms or fulfill social roles; a space where one can be herself, rather than an excellent employee, a friendly neighbor or a loving spouse.\textsuperscript{75} In the words of Supreme Court President Justice Barak in the \textit{Dayan} case: "In the hectic life of modern society, the right to privacy allows a person to be left alone and be with himself and with his loved ones, to gather strength at his home for the following day."\textsuperscript{76}

The right to privacy also enables to a large extent the \textit{freedom of speech}. The Freedom of speech is essential for one's self realization,\textsuperscript{77} the search for the truth,\textsuperscript{78} keeping public order,\textsuperscript{79} and it is one of the most sensitive issues in a democracy.\textsuperscript{80} Freedom of speech is not explicitly included in any Basic Law, unlike the right to privacy, but nevertheless, it has been recognized by the Supreme Court as a basic

\textsuperscript{72} Fried, \textit{supra} note 65 at 210-211.
\textsuperscript{73} Westin, \textit{supra} note 26, at 34.
\textsuperscript{74} Robert Maclver quoted by Westin, \textit{Ibid, ibid}.
\textsuperscript{75} \textit{Ibid}, at 34-35.
\textsuperscript{76} \textit{Dayan}, \textit{supra} note 30, at 470.
\textsuperscript{77} Freedom of speech allows each individual to form his or her own perspective which is the basis for spiritual and intellectual development (HCJ 399/85 \textit{Kahana et al v. The Israeli Broadcast Authority Management Committee et al}, 41(2) P.D. 244, 273).
\textsuperscript{78} Freedom of speech allows "various perspectives and ideas compete against each other. This competition - rather than governmental dictation of a single 'truth' - lead to the emergence of the truth … " - \textit{Ibid}, at 272.
\textsuperscript{79} Freedom of speech allows minority groups to "let out steam", and restricting untrue expressions may lead to a violent outburst of such "steam" (HCJ 316/03 Bakri v. Movies and Plays Censorship Commission, 48(1) P.D. 249, Judge Dorner, para. 9).
\textsuperscript{80} CA 255/68 \textit{State of Israel v. Ben Moshe}, 22(2) P.D. 427, 435. Freedom of speech allows for opinions to be voiced and exchanged; this is an essential condition for political and social regime (HCJ 372/84 \textit{Klapfer-Nave et al v. Minister of Education and Culture}, 38(3) P.D. 232, 238).
constitutional right.\textsuperscript{81}

The existence of the right to privacy encourages us to express ourselves freely. Privacy enables us to act in a way that may embarrass us if others knew about it;\textsuperscript{82} when we are being observed, we act differently;\textsuperscript{83} when others listen to our conversations we use a more formal language, which disrupts our ability to communicate in an honest and effective manner.\textsuperscript{84} If we are constantly exposed to the public eye, we lose our individuality, blend in with the crowd and our opinions will never be unique.\textsuperscript{85} Sometimes the mere knowledge that we are being watched or followed can cause a "chilling effect", causing us to censor ourselves and to avoid expressing ourselves altogether.\textsuperscript{86} Freedom of speech is of particular importance in the digital environment, where the passive media consumer becomes a user, who takes part in the process of creating an information environment. We discuss the relationship between freedom of speech and the right to privacy in the following sub-chapter, dealing with privacy on the web.

The harm to the freedom of speech is also detrimental to freedom of research. First, preventing free speech that may enrich the public discourse disrupts the flow of information. A free flow of information is essential in order to create new knowledge, created on the basis of existing knowledge. Secondly, one's knowledge that he or she are being flowed may deter one from searching, reading and receiving information on subjects of interests, for fear that the information collected about the subject may be misused.\textsuperscript{87}

The second class of justifications sees the right to privacy as a means for other interests. These interests draw several circles around the individual, from the

\textsuperscript{81} See HCJ 4804/94 Station Film corporation Ltd. v. Movie Censorship Committee, 50(5) P.D. 661, 675; CA 4463/94, 4409/94 Golan v. Prison Service, 50(4) P.D. 136.

\textsuperscript{82} Rachels, supra note 66 at 323.

\textsuperscript{83} Jeremy Bentham's Panopticon is a transparent prison, intended to make the control over prisoners more effective through constant observance by the warders. Following this concept, Michel Foucault claimed that control over people is achieved by their observance; the knowledge that they are being observed creates a discipline that renders physical force unnecessary. See Michel Foucault, "The Means of Correct Training", in The Foucault Reader 188-193 (Paul Rabinow ed., Harmondsworth, Penguin Books, 1984).


\textsuperscript{85} Bloustein, supra note 3, at 188.

\textsuperscript{86} See Fighting Terror Online, supra note 63, at 64.

\textsuperscript{87} Ibid, at 65.
relationships with those closest to him, to society and the community he is part of and the country he lives in.

On the personal level, the right to privacy enables equality and narrows the social divide. Privacy grants us the ability to hide certain details about ourselves that we know are likely to cause unjust discrimination against us. Thus, for example, when we look for a new job, keeping certain details private, such as our age, marital status or sexual tendency in our résumé opens the gate for us, giving us an opportunity to prove ourselves without prejudice. Furthermore, in a world without a legal right to privacy, the rich would have both the money and the means to protect their own privacy and the ability to violate other people's privacy by purchasing information they are interested in. Therefore, even if it can be argued that in the modern world privacy is only granted to the rich, while the poor are required to fully disclose private information in order to receive social benefits, the default situation of having no privacy at all will only worsen this situation.

On the social level, the right to privacy assists in developing friendship, love and trust in people's relationships.\textsuperscript{88} Psychologists and sociologists stress that life in society is only possible because each of us has the ability to present himself in a partial way and hide certain parts of his personality form society.\textsuperscript{89} Others maintain that the right to privacy makes intimacy possible, by dividing our personal relationships from the general public.\textsuperscript{90}

In addition, a private space allows people to accumulate power, leading to leadership. Not knowing all the details about our leaders makes it possible for us to trust them and rely on them. Privacy creates a knowledge gap which makes us believe the image that the leaders create about themselves. This does not mean that the government is not transparent, just that certain aspects of our leaders' lives are private.

On the general political level, privacy is an essential condition for the rule of the people, for democracy, for a free society. Privacy grants autonomy without which one cannot decide whether or not to accept the norms common in a certain society,

\begin{footnotes}
\item[88] Fried, \textit{supra} note 65, at 205.
\item[89] Gavison, \textit{supra} note 59 at 70; see Rachels, \textit{supra} note 66 at 323.
\end{footnotes}
from a critical point of view rather than blind obedience. Moreover, an informed decision reflecting the true will of the people can only be made in private, secretly and without outside influences.

A.5. Conflicting Interests

As we have seen, there are many substantial theoretical justifications for the privacy. However, as with any basic right, the right to privacy is not absolute. Under Israeli constitutional law, it must be balanced in each and every case against conflicting rights and interests. It appears that there is no dispute that we are willing to accept some violations of privacy, in order to maintain a proper balance between the right to privacy and other important interests.

The right to privacy may conflict with freedom of speech. The relationship between the right to privacy and freedom of speech is complex. As noted above, the right to privacy may encourage freedom of speech, as its very existence encourages people to express themselves. However, in many cases, the right to privacy prevents speech that violates privacy. In some cases such speech are technologies that have an enormous contribution to efficiency and progress. In other cases, the speech prevented may be newspaper articles that have an important social role. The freedom of the press, derived from the freedom of speech, enables independent open criticism of the authorities and realizes participatory democracy. Compromising freedom of speech also leads to the freedom of research being compromised, since the right to privacy places limitations on the ability to gather information, use it and adapt it.

Another right compromised by the protection of the right to privacy and derived from the freedom of speech it the public’s right to know what is said or done by others whose actions affect the public. This right is based on the view that the individual can form an opinion on things around him only if a wide variety of information is accessible to him, which may sometimes include information on other

---

91 Gavison, supra note 59 at 70.
92 On the relativity of the right to privacy see for example Dayan, supra note 30 at 480-481.
93 See Fighting Terror Online, supra note 63.
95 See Fighting Terror Online, supra note 63, at 66.
96 Segal, supra note 42 at 176.
people's matters. Thus, in some cases, invading one's private domain is considered part of the price one has to pay for being a part of society. Absolute protection of the right to privacy ignores the fact that individuals living in a society are co-dependent, a situation which justifies disclosure of private information in the "public interest" - where the public is substantially benefited by such disclosure.

Criticism of this kind is expressed by Professor Amitai Etzioni in his book *The Limits of Privacy*. Etzioni criticizes the liberal legal discourse that overemphasizes personal rights, at the expense of the common good. The right to privacy is an artificial concept, granting a social license to negative behavior such as lies, hiding important information and avoiding responsibility for one's actions. According to Etzioni, a person living in a society has no right to privacy in certain situations, where hiding information is detrimental to the public need for security and health (such as the confidentiality of the names of people with AIDS or criminals found guilty of sexual abuse of children). Conceptually, Etzioni argues that in these cases there is no conflict between one's right to privacy and the public interest. In his opinion, these are situations where the right to privacy does not exist at all.

The right to privacy may also conflict with the public interest in law enforcement, essential for the protection of our basic right to protection of freedom and personal security. Under the veil of privacy one can act illegally, without the state having the ability to follow his actions. This conflict becomes more substantial as technology progresses, as the possibilities of monitoring one's moves and actions increase and become an efficient and important tool in the war against crime and terrorism. We shall elaborate on this issue in the next chapter.

Weighty arguments against the right to privacy are also heard by the economic analysis of the law. An economic analysis of the right to privacy may lead to the conclusion that this right is inefficient, as argued by Judge Richard Posner.

---


98 The "public interest" is different form "of interest to the public" which can be any subject of interest to a person, even if only sue to curiosity or gossip (*Ibid*, at 193-194).


100 *Ibid*, 185.

101 Lecture by Professor Amitai Etzioni (Haifa Center of Law & Technology, 11 January 2004).


103 Posner, *supra* note 84.
relies on two basic assumptions. First, that privacy inhibits the flow of information, while full information is a condition for the existence of a perfect market and second, that information is an economic resource that can be traded, therefore it should not be subject to limitations such as privacy.\textsuperscript{104} Privacy protects only the liars, those who have something to hide. In his opinion, there is no difference between a trader who misrepresents his goods and a person who hides personal details in order to improve his social and business connection. Therefore, each of us has the right to expose information hidden by others, in order to create an accurate picture of their character and to protect ourselves from unsuccessful relationships.\textsuperscript{105} Hence protection of privacy is justified only in cases where it is essential in order to give people incentives to create more information (for example, protection of trade secrets) or where the violation of privacy compromises the quality of the information (for example, eavesdropping on others' conversations).\textsuperscript{106} In instances where the right to privacy will increase the costs of transaction reduce welfare, this right is unjustified.\textsuperscript{107}

Another approach is raised in a book by Professor Niv Ahituv, \textit{A World without Secrets}. Ahituv suggests that the information in the modern age should be open and accessible to all.\textsuperscript{108} He argues that complete protection of databases open to the public is impossible, and even if it can be done, this is a complex and expensive solution. Therefore, resources should not be wasted on protecting information - we ought to join the "open information society", where the protection is limited to those few pieces of information that must be protected.\textsuperscript{109} Ahituv claims that our old values should adapt to technological changes.\textsuperscript{110} Therefore, he calls for a renewed discussion on the extent to which the right to privacy is suitable for today's society, based on the assumption that privacy is no longer a scared cow.\textsuperscript{111}

Another criticism on the right to privacy is raised by feminist theory. One of the continuous and most well known feminist struggles is against the tradition liberal

\textsuperscript{104} Ibid, 336-339.
\textsuperscript{105} Ibid, at 337-338.
\textsuperscript{106} Ibid, at 341.
\textsuperscript{107} Ibid, at 339.
\textsuperscript{108} Niv Ahituv, \textit{A World without Secrets - On the Open Information Society} (Tel Aviv, 2002).
\textsuperscript{109} Ibid, at 56-57.
\textsuperscript{110} Ibid, at 118.
\textsuperscript{111} Ibid, at 118-123.
distinction between "private" and "public", as this distinction grants men an advantage and perpetuates the inferior status of women in the private sphere. The reason for this is that women are kept out of the public sphere and are required to limit themselves to the private sphere: raising children and running the household. At the same time, men enjoy control over the private sphere, where they can control women, sexually abuse them, beat them and even rape them. In fact, the policy of non-intervention with private lives enables men to harm women far from the public reach and outside the rule of the law.

A.6. Interim Summary

It is difficult to define the right to privacy, since privacy is not a pure legal term. It has psychological, social and political aspects. The conceptual difficulties in defining the right to privacy are caused both by the fact that various interests protected by the right to privacy are also protected by other laws, and by the fact that the right to privacy is affected by political, social and economic changes and by technological developments. After reviewing the various definitions of the right to privacy in the case law and in academic literature, it is possible to formulate a definition which includes both the access and control elements:

_The right to privacy is our right to keep a domain around us, which includes all those things that are part of us, such as the body, the home, the thoughts, the feelings, the secrets and the identity. The right to privacy gives us the ability to choose which parts in this domain can be accessed by others, and control the extent, manner and timing of the use of those parts we choose to disclose._

Theoretical justifications of the right to privacy are required in order to face technological, social and other changes and to draw the borderline between the violations we wish to prevent and those we can allow, so as to protect another interest. One type of justifications sees the right to privacy as an end in itself: these justifications see the right to privacy as a means for realizing human autonomy; for keeping one's peace of minds; for encouraging freedom of speech, which can be violated if one knows he is being watched or that his conversations are tapped, and for

---

112 Orit Kamir, _Feminism, Rights and the Law_ (Tel Aviv, Ministry of Defense, 2002), 72-73.
113 _Ibid_, at 74.
114 _Ibid_, at 75.
protecting freedom of research, i.e., the ability to search, read and receive information without fear. Another type of justifications sees the right to privacy as a means for achieving other interests: equality and narrowing the social divide; encouraging companionship, love and trust in people's relationships; allowing for the accumulation of power, leading to leadership; the ideal of the rule of the people, democracy and free society.

There are many substantial justification for the right to privacy, yet there are certain limitations of privacy that we are willing to bear, in order to maintain a proper balance between the right to privacy and other important interests. Like all other basic rights, this right is not absolute. Such interests may include the freedom of speech and the public's right to know, law enforcement or economic interests, harmed by the lack of full information and the limitations on trading the privacy resource.
B. Privacy on the Web

B.1. The Digital Environment and the Information Revolution

There is a revolution, and though it may be quiet, it is well felt by every person in every day life... the Internet is, on the one hand, only technology, but on the other hand, a cultural revolution, maybe also a social revolution. New technology necessarily creates new law.\(^{115}\)

In this sub-chapter we address the difference between the approaches to privacy in the physical environment and in the digital environment; we examine the change in the definition of privacy and its extent, we discuss the changes in the possibilities for violations of privacy and the changes in the ability to obtain privacy; we focus on the characteristics of the information revolution, enabling the violation of privacy in the digital environment in general and on the Internet in particular.

The right to privacy changes with technological progress. While in the past there was a need to protect only the most sensitive and intimate pieces of information, such as one's sexual behavior, medical condition etc., nowadays it seems that privacy should also be protected with regard to consumer behavior, name, address, date of birth, marital status, looks, occupation and so on. This is due to the technological changes, enabling data crossing processing and creating a personal profile based on simple details, which on the face of things we have no interest in protecting.\(^ {116}\)

During routine activities we engage in, such as electronic correspondence, purchases by credit card and other such simple activities with an electronic element, we provide various bodies with information about ourselves. Providing this information is done with our supposed consent and we do not fear that our privacy may be violated as a result. In practice, such "public" information, which is not intimate or particularly sensitive, is gathered and collected together with other pieces of information, seemingly useless for the purpose of monitoring or following us, and it is analyzed and sold.\(^ {117}\) At the end of the day, the use made of all the information gathered about us may violate our privacy, enable various bodies to invade out "personal" computer, flood our e-mail boxes with enormous amounts of information,


obtain information about us which we had no intention of giving to such bodies and so on.

Before the digital environment evolved, the ability to violate one's privacy was limited, as was the ability to maintain privacy. The digital environment removed many of these limitations. The objective circumstances of overcoming crime and terror and as a result the decline in personal safety, increased the need for developing means of surveillance and the use thereof: fingerprints, detectors for bodily checks and various monitoring and tapping devices, with the declared objective of granting us protection, and for this objective we assume that most of us are willing to permit a certain invasion of privacy. Once the technology is developed, its use can no longer be restricted only to the objectives for which it was developed, and nowadays it is also being misused, both by the authorities and by individuals.

In the past, protection from invasion into a large physical domain required substantial personnel or was impossible for technical and/or economic reasons. These days a "smart camera" can be installed, or a satellite can be used in order to secure large areas, to the extent of protecting national borders, as in the United State.118 It should be noted that the means of protection against privacy violations are becoming more sophisticated, but as the arms race continues, the gap grows between those who can afford sophisticated means of protection and those lacking in means who are left exposed. This is true especially in view of the rapid development of technology, compared to the slow progress of the legal system which may reduce this gap.

"Technological means in the freedom of information age have brought the discussion on the right to privacy to new levels. Invading one's privacy no longer requires reaching his house and looking through his personal effects. These days, invasion of privacy is one click away."119 In one of the following chapters we examine in depth and in detail various means of surveillance in the digital environment.

Most of the violations of privacy in the digital environment are due to use of new technology, enabling aggregation of an enormous amount of information on an unlimited number of people, reproduce this information at minimal costs, transmit and

118 David Shneck, "You are being Followed", 66 National Geographic (November 3002), 10 (hereinafter: "You are being Followed") (Hebrew).

119 See Fighting Terror Online, supra note 63, at 61.
trade it, in a manner that does not involve costs of storage, transport etc. In addition, data mining programs can sort and categorize data, which make it easier to use it in a way that can serve many purposes and bodies, as well as algorithms for data mining.

In order to better understand the future of privacy in the digital environment, we should examine the relevant characteristics of the web.

B.2. Awareness, Anonymity, Ease of Use and Absence of Boundaries
The strength of privacy is directly affected by technology. In a world without computers, cameras, microphones, satellites and knowledge on fingerprints and genetic information, privacy would have been stronger. In this section we seek to clarify some of the characteristics of the web that influence the extent of the right to privacy. These are not necessarily technological, but social practices developing around the technology. We examine in particular the users' awareness, a question which is also linked to the element of consent, the anonymity of use, accessibility and the absence of boundaries.

1. Awareness
Since the rate at which technology develops is so fast, it is almost impossible to follow the changes, and apparently this rate will only speed up in future. Most people, even those who are familiar with computers, are not aware of the implications of their naïve use of the web, where they in fact waive their rights, without being aware of it, in the course of their day to day use of various electronic services offered to them. This is particularly true with regard to that part of the population that was not "born into" the world of information and computers, does not know this field and obviously is unaware of the implications of databases, gathering information, analyzing it and cross processing information. Since the violation of basic rights such as the right to privacy is unbearably easy in the information age, the public ought to be informed of such violation of privacy. In this sense, the web is essentially different from the physical environment.

In the physical environment when one's privacy is violated, she is normally aware of the violation, feels it and has legal and other tools for dealing with it (by preventing the violation by greater protection of her privacy, a legal action for compensation or other means). In the digital environment, when one is exposed to various privacy violation, and she is unaware of the extent of her vulnerability, it is
harder to prevent the violation and the legal protection against such violations should be much wider, in order to prevent a situation of absence of privacy (assuming this value is protected by the state and by society).

2. Anonymity

The digital environment has many opportunities for anonymous electronic interactions. The physical nature of distant communication, while hiding behind the computer screen, the technical difficulty for the average user to expose the true identity of the user and the lack of legal and/or social norms forbidding anonymity online, all of these factors allow the user to remain anonymous. A person can send e-mail, participate in discussion forums and voice his or her opinions in chat rooms, purchase products for "cash" on different sites or simply surf the net, without identifying or revealing the real name. As a result, public discourse is enriched, including views and information which would not have reached the public had the speakers been required to reveal their identity.\textsuperscript{120} Anonymity makes it possible for users to express their opinions without fear of the need to explain, give reasons and be punished for using a certain expression, be accountable or apologize. Anonymity makes it possible for us to act confidently, openly and without reservations. Without the fear of being examined or judged by others, we have freedom of thought, freedom to develop arguments which perhaps we would not have expressed openly, for fear of hostile criticism from close associates or other pressures. In these aspects, anonymity serves the freedom of speech and basic individual liberty. Moreover, in many cases thanks to anonymity we are not afraid to express ourselves or call for help, especially where our problems cause us embarrassment or shame, due to social stigmas, such as some diseases, or psychological problems or economic difficulties, or for other reasons.

Despite the many advantages mentioned, anonymity has many disadvantages. It allows for avoidance of responsibility for illegal and/or immoral online activities. Copyright owners face great difficulty in monitoring violators on the web, the web provides a convenient base for fraud and impersonation, as one cannot tell who he is communicating with on the web, for example in entering into contracts, interpersonal interaction, giving seemingly professional advice and spreading rumors and

\textsuperscript{120} Ibid, at 65.
defamation. In this way, national secrets may be revealed, people may conspire to commit crimes or aid them and pedophiles can seduce minors to meet them. Furthermore, information that has no source cannot be relied on, which renders trustworthy information doubtful.\textsuperscript{121}

Since anonymity allows for searching for information and spreading it, dangerous information becomes accessible to anyone. The lack of supervision and the anarchy typical of the web contribute to the growth of a wide terrorist network, which could not have grown under different circumstances. For instance, the unbearable ease with which one can obtain information on preparing explosives out of readily available materials, coupled with the ability to get information on vulnerable places anywhere in the world make it easier for terrorists and make it extremely hard for the law enforcement officers. However, anonymity can also be a convenient and useful tool for finding those who wish to harm national security and spy after them. It should be noted in this context that as the web develops, a new type of criminals is emerging, whose weapons are the digital environment and the world of computers. Despite the development of technology enabling monitoring, the criminals who master the web can leave no traces, and in this case the ability to enforce the law and prevent crime is close to zero.

Anonymity, by definition, means remaining nameless, acting without revealing the name of the actor. Anonymity is essentially the ability to be unreachable, to be free of pressures such as the duty to be accountable, explain, give reasons, apologize or be punished.\textsuperscript{122}

It is well known that anonymity is an essential element on the Internet. This is only seemingly true. In the information age, the problem is that despite the ease of maintaining anonymity, it is not clear whether the aim for which anonymity is protected is in fact achieved. Technology enables following people with incredible ease, anonymity is no guaranty for privacy.\textsuperscript{123} Even if the user does not reveal his name, many details about him are gathered through different interactions while he surfs. Collection the pieces of information can identify him despite his attempt to maintain his anonymity. The main argument raised by Professor Helen Nissenbaum is

\begin{flushright}
121 Lecture by Dr. Naama Carmi, Neve Ilan Conference, 17 December 2003.


123 Lecture by Dr. Yuval Elovici, Neve Ilan Conference, 17 December 2003.
\end{flushright}
that in order to achieve anonymity a great deal of effort is required, even more than for hiding his name. If, as a society, we recognize one's need to be untraceable in some circumstances, we should act towards protecting confidentiality of personal information. Most users believe that the web grants them anonymity. Although in practice the user is not anonymous, his lack of awareness of the true facts grants him the "protection" of anonymity, allowing the user to "use" all the advantages of online an, as described above.

Should anonymity in itself be protected? In Israel the courts have not yet recognized anonymity in itself as a value worthy of protection. In the *Borokhov* case, Judge Amir stated as follows: "Anonymity on the Internet is not a moral or ideological matter, but a fact resulting from the absence of prohibitions and from distant communications and the technical difficult in exposing the true identity of the user. However, as this anonymity has no protected value, we should not invent protections for it." According to Judge Amir, the Internet symbolizes freedom and anarchy and for this reason, apparently, the legal in the digital environment should be minimal and limited to acute matters of personal privacy, such as intercourse, sexual preferences and health matters. Dr. Yuval Karniel argues that these days, when norms are changing and there is little shame, there is no longer a need to protect anonymity. In his opinion, the public these days has seen and heard everything, therefore it is tolerant and open and willing to accept those who are different, unusual, perverse and weird. People run their intimate conversations in public and do not even bother to lower their voices. Therefore there is no point in wasting energy and public resources on protecting interests that the public is indifferent to, and it does not appear that their protection is at the top of its list of priorities.

In the US the key ruling on this issue states that anonymity in itself is a protected value and this protection can be removed only when certain conditions apply. The case that so determined dealt with revealing the identity of users by the internet service provider (ISP) following their inappropriate conduct which caused harm to other users. The court set three conditions and only when these apply will the

---

124 Ibid.
125 TA (Tel Aviv) 7830/00 *Borokhov v. Poran* (unpublished; decided 14.07.2002 )
126 Lecture by Dr. Yuval Karniel, Neve Ilan Conference, 17 December 2003.
service provider be obliged to reveal the identity of the users, as follows: 1. initial evidence indicating harm; 2. the ISP was approached in good faith and for a justified reason; 3. it is essential to reveal the identity of the users.

We must not forget that when we discuss anonymity, we discuss an aspect of privacy. In our opinion, anonymity is not only a means for achieving privacy, but due to the advantages mentioned above, it is a value worthy of protection in itself. As long as it is not misused, it ought to be protected. Hence, we consider that the American approach is the appropriate one, because it strikes a balance between protection of anonymity for positive purposes and removing the protection when it is misused in order to cause harm to others.

3. The Ease of Use

Technological progress and the development of video cameras and various means of surveillance and tapping enable expression through home videos and creating a virtual reality in the style of *The Truman Show*. The availability of the technology and the natural curiosity on the one hand, and the clever media, feeling the public pulse and aiming at maximizing the viewers' ratings on the other hand, have brought along a wave of reality TV shows, movies and media events. This phenomenon is even more evident on the web, in the absence of editing, censorship or ethical codes of the press, that may limit or prevent the harsh expression which may violate privacy. Furthermore, every end-user can, with little effort and cost, upload his creations and distribute them. Consequently, there are phenomena such as home porn videos, photo-montages in famous people's porn movies, publication of people's photos without their consent and spreading rumors and gossip. These phenomena are only examples of a rapidly developing genre. Controllers of the media who seek higher ratings encourage participation in shows of this kind, through various incentives (advertising, money, gifts etc) and encourage crude violations of privacy. This may diminish the value of privacy in the public opinion.

The technological means and the availability of the new medium and the ability to express oneself in an unlimited way online turn every end-user into a potential reporter. For example, during the "Defensive Shield" military operation in April 2002, IDF soldiers, using cell phones, served as a news source from the
battlefield. The same thing happened during the September 11 terrorist attacks and the crash of the Columbia space shuttle.

Prior to the digital age, privacy was protected from harm caused by advertising in two ways: first by prevention, through the ethical code of the press, and secondly by punitive measure, by the law. Nowadays the preventative aspect has been weakened to such an extent that it can be said to have disappeared completely on the web. The result is that the tools used in the physical world cannot prevent in advance violation of privacy due to publications on the web, and imposing sanctions on violators on the web also involves considerable difficulties, as described in the previous chapter.

The ethical code of the press does not apply to end-users, and in fact neither does it bind online journalists. But while journalists usually abide by the code voluntarily, due to the prestige of the press council and its public influence, the end-users do not and are mostly unaware of the existence of this code. Consequently, the end-users publish rumors and items that are baseless and have not been checked and new items are published before the time is due (for example, by ignoring an injunction barring publication or publishing the name of a deceased person before his family has been informed). Such publications may violate privacy and cause irreversible damage.

4. The Absence of Boundaries
One of the main characteristics of the Internet is globalization. Almost unlimited technological means enable the evasion of the various arrangements relating to privacy. As long as the whole world is not in agreement with regard to the extent to which privacy ought to be protected, if at all, there is no way one law can be imposed in all states in which the web is used. Therefore, public regulation, namely regulation by legislation, is problematic. However, private regulation exists, namely regulation by private bodies developing various technologies in order to protect online privacy.

---

129 The Press Council cannot impose the code of ethics on journalists who so not wish to follow it, but the prestige of the commission and its public influence, leading journalists to adopt the code of ethics, cannot be disregarded.
130 See the decision of the Press Council of January 3002 to apply the code of ethics to "online journals".
The market forces and the technological race determine the extent to which privacy is protected at any given time. In the following sub-chapter dealing with Internet regulation we discuss these issues in length.

The Internet, being a public sphere, belonging to all of us, creates a potential that is greater than ever for phenomena that violate privacy and are not regulated by the law. Monitoring the site to which we surf and gathering information on the type of computer we use or on our IP address do not invade our physical space where we have property rights. It also appears that it would be hard to define them as violation of privacy that violates human dignity.\textsuperscript{131}

\textbf{B.3. A Renewed Ethical Examination of the Appropriate Balance between the Different Values in the Digital Environment}

Following our discussion on the theoretical basis of the right to privacy, we now deal with the relationship between privacy and other values on the Internet. We shall focus on those components and consideration in which there has been a change in the digital age, due to technological developments in general and the Internet in particular. In the Workshop position paper of 2002 Fighting Terror Online, we discussed in length the conflict between security needs and the right to privacy and therefore we shall not discuss it here. We shall examine the values compatible with privacy and those conflicting with it. We shall consider whether the extent of protection of the values worthy of protection in the physical environment, as detailed above, is widened, narrowed or remains the same in the new technological environment? And to what extent should we protect privacy on the Internet?

\textit{Privacy and Freedom of Speech: Technology created a new reality} in which everyone can voice her thoughts on the web and sometimes evade sanctions. Although the system of checks and balances in the physical world with regard to the balance between the freedom of speech and other values, such as privacy, is still appropriate in our view, and we want to maintain the same "proper" balance in the digital environment, we find that this is impossible, since the existence of the web creates a new reality. In this reality, our efforts to balance using the same means are bound to fail, as they are incompatible. For example, issuing an injunction barring publication in Israel with regard to information, even if we agree that such

\textsuperscript{131} We discuss this in the second chapter on means of surveillance.
information should not be disclosed (in order to protect privacy, for example), is an ineffective measure for achieving this result. Such an order can easily be evaded, by uploading the information to the web outside Israel, and thus no offence is committed.

Freedom of speech is particularly important on the web, therefore a new examination of the balance between the freedom of speech and the right to privacy is called for. Dr. Yuval Karniel is of the opinion that in the digital age, there is no room for a sweeping protection of privacy, since the public's list of priorities has changed, a new list must be recognized and this does not consider privacy as a value worth of protection. Many believe that since the Internet is the "home court" of freedom of speech, it should be given priority on the web. According to Professor Niv Ahituv, since the Internet is a new environment, it should be subject to laws that are compatible with it, in order to invest resources in an efficient manner, rather than impose the old norms which are incompatible with the characteristics of the new environment. Ahituv considers the Internet to be the open information society, namely, almost all types of information should be available to everyone, at a reasonable price. This approach sees freedom of speech as highly important, even at the price of privacy violations.

The web serves as a stage for anyone who wishes to use it and an endless source of information on any subject. Seemingly the Internet grants the individual unprecedented power for delivering messages. Any person can express himself on any topic at minimal costs and with incredible ease. Moreover, it appears as if the most reliable and up to date information in any field can be found on the Internet and as if the control is in the hands of the user, with regard to the information he is exposed to the search process and the types of information providers. In fact, these are myths. The technological infrastructure of the Internet does grant every end-user the ability to express himself on the web easily and at a minimal cost, since technically, there are more than a few central points creating a bottleneck for all online expression. However, the structure of the web and the myriad of users create many

132 Lecture by Dr. Yuval Karniel, Neve Ilan Conference, 17 December 2003.
133 Niv Ahituv. A World without Secrets - On the Open Information Society (Tel Aviv, 2002).
134 Ibid.
decentralized stages, so the user may only have a very small audience, if any. As a result, the unlimited extent of freedom of speech on the Internet is only theoretical. With regard to the second myth, firstly, not all information available on the web is reliable, since there are no filters and any end-user can distribute information as he wishes; and secondly, the Internet market is ruled by powerful private bodies, exploiting psychological elements of users for the purpose of promoting their economic interests, as detailed below. Therefore, the end user is manipulated in the search process, the order in which information reaches him and the types of information. Thirdly, due to the enormous amount of information on the web, the end-user suffers from information fog and cannot find the relevant search results - he must define with great precision the information his searches for and focus on it.\(^{137}\)

It is therefore impossible to estimate the extent of the violation of privacy due to expression on the web. On the one hand, the violation may be smaller than it appears, in light of the decentralized stages, On the other hand, despite the decentralization, one can never trust that the violation will be slight, as the information is available and accessible to every user and we never know who will access it.

The balance between privacy and the freedom of speech requires us to treat information as property, but in a very different sense than what we are used to. On the one hand, personal information can be classified as the property of those who trade in it. There is no conflict between the trader's right to control its own property and use it as it sees fit and between freedom of speech. On the other hand, information can be classified as the property of the individual to whom it relates. We have to balance between the freedom of speech of the trader and the individual property right.\(^{138}\)

Privacy vs. The Private Market Forces: collectors of information in general and of personal information in particular are not a new phenomenon. However, the digital environment raises grave concerns about the social and personal uses of these databases in digital format, enabling a fast search, immediate distribution and data crossing, creating a comprehensive personal list including characteristics and consuming habits.\(^{139}\) Private bodies having money and power are willing to trade in these databases and claim that the information collected and adapted by them is their


\(^{139}\) *Ibid*, at 1374.
property.\textsuperscript{140} Centralized power in the hands of the private market creates a conflict between the economic possibilities of the large private bodies, especially through advertising and marketing online, and the ability to protect the innocent user who exposes himself and information about them to those bodies, without being aware of the implications involved. Lack of privacy protection prefers the freedom and efficiency of these private bodies to the freedom and efficiency of individuals in society.\textsuperscript{141}

The danger involved in the existence of private databases is that their owners are not subject or the same public criticism and the same standards and rules of proper administration. Private bodies can pass the information over to anyone who wants it or willing to pay for it and we have no control and/or guarantee that the information does not reach dubious, malicious or hostile hands. Moreover, we have no idea, let alone control, of who has information about us. This new threat increases he need for strong protection of privacy in the digital environment.

As noted above, strong corporation can influence our ability to control the information we are exposed to on the web. If we define the right to privacy as including one's ability to control the information that reaches him, such influence can be considered a violation of privacy. Since the profits of the owners of a private website grows with the number of users who visit the site and are exposed to the advertising sponsoring it, the site owner is willing to pay search engines in order to appear on the top of the list of search results. The natural tendency of the average user is to click the links of the sites at the top of the search result page, therefore it is highly probable that the user would visit that site. The result of this economic model is that the list of search results represents the sites that paid more, and is not listed in an objective order, for example in accordance with the quality of information appearing on that site, which is particularly relevant to the searcher. The user's privacy is violated when she is denied her freedom through psychological manipulations and denied an efficient search which she could have had if the search engines were to produce objective and effective results.

\textsuperscript{140} Ibid, at 1376.

\textsuperscript{141} Ibid, ibid.
B.4. Interim Summary

In the context of privacy, the technological developments have created a new reality, on both the legal and the practical level. While technological progress has changed the rules of the game completely, the legal system lags behind. While lawyers are still thinking over the appropriate form of regulation and its appropriate boundaries, the violators of privacy accumulate knowledge, power and information and impose norms of conduct which will be almost impossible to uproot. A reality where there is no law and order raises the question - is it still possible to protect privacy? All of these issues lead to legal questions about the appropriate realm of the right to privacy and the choice of the best form of regulation. The users' awareness is a central question, and in light of the definition of privacy we have suggested in this position paper. Consent is the subject of the third chapter, but first we examine the options for regulation.

B.5. Regulation

In this position paper we attempt to examine whether we can handle the threats to privacy created by the digital environment. The threats we focus on are those created by the private market, rather than those created by the state. In the past, the main threat to the right to privacy in the digital environment was indeed that of Big Brother,142 but these days it appears that the "little brothers" are the ones posing threats just as severe. When it comes to threats by private bodies, the question of regulation is all the more valid, since these are not subject to constitutional or administrative duties which can restrict the power of the state. In the various chapters of this paper we raise different options for handling these threats each formulating technology in a different manner: public regulation, private regulation and indirect public regulation.143

With regard to any threat presented in this position paper we shall ask is it appropriate to intervene and regulate this phenomenon. If we reach the conclusion that it is, we shall try to examine the appropriate means of intervention and its appropriate extent.

Our basic assumption is that we must not surrender to technology that enables new violations of privacy. Some consider that technology has fundamentally changed

---

142 This threat was the subject of the interdisciplinary Law and Technology Workshop in a previous position paper. See Fighting Terror Online, supra note 63.

reality and that the law must adapt its values to the new reality. This argument is based on modern culture that prefers exposure to privacy, in a reality where people conduct private conversations in public, get exposed on reality shows on television, sell their privacy in exchange for discounts, free surfing or club memberships. In this reality of no shame, no boundaries and no norms, protection of privacy is no longer justified. Therefore, the gap between the declarations on the "importance of privacy" and the low weight we give it in practice ought to be narrowed.

Another view maintains that those who are interested in participating in the digital revolution should come to terms with the violation of the right to privacy, which forms an integral part of the information environment. It seems that this position is based on technological determinism, according to which the de cannot be regulated at all in view of its "essence" and "nature" that cannot be altered or controlled.

We think differently. As Professor Lawrence Lessig wrote: "[H]ow cyberspace is is not how cyberspace has to be, there is no single way that the Net has to be." In his opinion, the Internet does not have an "essence." Technology is designed by human beings in order to serve human beings living in a social environment. Therefore, technology can be regulated and adapted to our values in the physical world. Lessig argues that the web can be regulated if we build an 

architecture that allows it, the architecture creates the contents. The term

144 Dr. Yuval Karniel, lecture at the Neve Ilan Conference, 17 December 2003.
145 In Israel these plans developed from exposing intimate moments to the camera to a total exposure of persona life with cameras accompanying a person throughout the day. Dr. Karniel says that this phenomenon attracts many people who have aspirations of developing a career in acting or modeling (Ibid).
146 Ibid.
151 Ibid, at 6.
152 Ibid, at 25, 27. Lessig argues that the "nature" of the Internet that makes it impossible to regulate is changing.
153 Ibid, at 8.
"architecture" refers to the technological structure of the web and the applications installed at the ends of it. The architecture of the web can be built so as to regulate conduct that does not violate privacy, but for this to happen there must be legal incentives. The right to privacy should be the default option, when the role of the law is to regulate negotiations between the individual and technology, allowing him to waive this right in certain cases.

Indeed, in the digital environment the world of legal values has been altered. Technological characteristics are only an integral part of any balance of conflicting interests and in many cases they will determine the arrangement to be created, therefore we shall not attempt to subject technology to the legal rules in an arbitrary manner, but to combine them, realizing the advantages of technology and understanding that it may be that some of the values that the law sought to protect traditionally should be adapted to technology.

1. **Direct Public Regulation**

One possibility of regulation of privacy violation on the web is public regulation. Public regulation may be achieved through implementing the general law of the physical world to the digital environment, or through setting new legal rules, formulated by the legislator, the courts or the government. These rules may be normative rules, clarifying what is allowed and what is prohibited with regard to privacy on the web, or technical rules imposing a duty on companies to use only certain technologies that do not violate privacy.

Public regulation of the digital environment has the advantages of transparency; laying the value considerations on the tables allows for public criticism and appropriate judicial review. Moreover, public regulation assists in ensuring legal certainty, assuming the law is comprehensive enough and does not require frequent amendments. In addition, public regulation grants a moral approval to the

---

155 Ibid, at 160.
156 Ibid, ibid.
protection of privacy, as a right that is central and important enough to be protected by the law of the state where such a law is enacted. Thus, for instance, a solution for a country where there is peace and internal stability cannot serve as an example for a country whose existence is under threat.\footnote{See the Report of the Committee on Protection of Privacy, supra note 2 at 89.}

Apparently, imposing legal rules on the Internet solves the problem of privacy violations in an immediate and efficient manner. However, we must remember that public regulation that we encounter in every field of life is not to be taken for granted when it comes to the digital environment. Many activities are not regulated by any legal rules, even if they violate interests that the law protects in the physical environment. The case law in Israel has already recognized the digital environment as a "new animal" that should not be subjected to the rules of the games that apply in the physical world.\footnote{In the case of \textit{Shas v. Piness} the chairman of the central election committee, Justice Cheshin, held that an analogy from the laws applicable to television and radio and the Internet is inappropriate as there is an essential difference between them: firstly, television and radio broadcasts are regulated by law while the Internet is not; secondly, the television and radio frequencies are limited, whereas on the Internet there is no lack of resources; thirdly, on television and radio the choice is much more limited than on the Internet; fourthly, television and radio users are passive while Internet users are in some sense "player"; furthermore, there is a difference in the speed of traffic, availability of service, simplicity, ownership and the array of services provided. This decision follows the American case of \textit{Reno v. American Civil Liberties Union}, 521 U.S. 844 (1997).} However, perhaps public regulation that is adapted to the web is inevitable where the courts apply the existing law, which does not fit the digital environment.\footnote{Adv. Tana Shpanitz, Deputy Attorney General, lecture at the Haifa Law & Tech. Workshop on New Copyright Legislation in Israel, Neve Ilan, December 11, 2002.} This is not the situation in Israel, where it is not common to apply general law provisions on privacy protection to the digital environment.\footnote{See for example CA 70868/00 State of Israel v. Elad Ben Yosef Baruch (applying section 30 of the Communications Law 1982, Laws of the State of Israel 218, prohibiting the use of a device "in a manner that may unlawfully cause harm, fear, harassment, anxiety or annoyance", in relation to a defamatory e-mail sent to a politician); BS 6703/00 Netvision v. IDF (unpublished) - the application of the Secret Monitoring Law to materials on an ISP's servers; TA 7830/00 Borokhov v. Poran - applying the PPA to a disclosing an Internet nickname).}

\textit{The main disadvantage} of imposing legal rules on the web, namely, state intervention in the virtual market, is compromising the freedom typical to the digital environment. On the web there is great potential for decentralized public discourse, open to a large number of participants. This potential exists due to the technological infrastructure, the unlimited channels do not entail the concentration of control in the hands of few media owners, the costs of distribution of information are low and the communication between the speaker and the audience is direct, without mediators
who may limit it or alter its contents.\textsuperscript{163} The decentralized nature of the web is essential in order to protect many diverse interests.\textsuperscript{164} Some of these interests conflict with the right to privacy (such as the freedom of speech, freedom of research and the public's right to know). And others justify it (such as realizing individual autonomy, personal development and an open and free democracy). Imposing legal rules on the web may have a chilling effect on the decentralized public discourse on the web.\textsuperscript{165} It is likely that many providers who will not consider operating the new mechanisms required by the law will have to reduce and even stop providing their services, due to the risk they involve.\textsuperscript{166} The remaining providers will have power and control on the web and thus the public regulation will lead to centralization on the Internet.\textsuperscript{167}

Public regulation may also have economic implication on the content providers, who will be under duty to set up mechanisms for filtering and editing contents and apply surveillance and legal advice. Therefore, only those with financial strength will survive in the market and they will have the power to design the contents of the information environment.\textsuperscript{168} Another possibility would be to make the users bear the costs of public regulation. As a result, the prices of service will rise and the number of users will decrease.\textsuperscript{169}

Rules imposing legal responsibility will affect the behavior of the players acting in the digital environment, change the characteristics of the discourse unique to this environment and compromise freedom of speech.\textsuperscript{170} Professor Yochai Benkler argues that keeping the digital environment free for everyone is essential especially at this point in time, when determining the control over the flow of information may design the web. In his opinion, public regulation of digital communications means copying the hierarchies already existing in the physical world; this grants those in power the ability to dictate how the future should look like. Therefore,

\begin{thebibliography}{9}
\item \textsuperscript{163} Niva Elkin-Koren, "New Intermediaries in the Virtual Public Forum", 6 L. & Gov. in Israel 365 (2003) (Hebrew).
\item \textsuperscript{164} Ibid, at 415-420.
\item \textsuperscript{165} For example imposing liability on ISPs for the publication of harmful materials by users would force them to use filters which may also block innocent materials. Ibid, at 389-390.
\item \textsuperscript{166} Ibid, at 392-393.
\item \textsuperscript{167} Ibid, at 383.
\item \textsuperscript{168} Ibid, at 393.
\item \textsuperscript{169} Ibid, ibid.
\item \textsuperscript{170} Ibid, at 406.
\end{thebibliography}
communication regulation in the 21st century must focus on contributing to the creation of more knowledge. Rigid legal restrictions will hinder the ability to do so and stop the information flow.\textsuperscript{171}

Another disadvantage of public regulation of the web is that it can subject technology to social values through the law. Such an attempt is in many cases bound to fail. The digital environment has an ability to change rapidly and constantly and a legal rule is born in a slow and complex process. If we create normative legal rules for regulating the digital environment it will be hard to adapt these rules to the changing expectations of the public, even if they try to formulate these expectations by long term vision. An example of this disadvantage is the Computer Law of 1995\textsuperscript{172} that was the product of a long legislative process and its final version does not refer to the Internet. If we create technical legal rules we will not be able to handle the ability of the technology to adapt itself to the legal rules and defend itself against any attack.\textsuperscript{173}

It appears that public regulation will not solve the threats to privacy at all or it may eliminate threats only for a short and insignificant period of time. Therefore in areas where new problems arise, we had better wait for norms to crystallize, watch the natural development of things, so that the technological race does not turn the law into an empty shell.\textsuperscript{174} Another partial solution is to adopt of a model of an existing law in another country and following its implementation and interpretation.\textsuperscript{175}

A third disadvantage of legal rules is that even after they are set, they depend on the ability to enforce them and on the resources invested in their enforcement.\textsuperscript{176} Law enforcement is costly and this is one of the considerations determining whether its enactment is worthwhile.\textsuperscript{177}

A fourth disadvantage is that public regulation operates mainly on the national


\textsuperscript{172} Laws of the State of Israel 366.

\textsuperscript{173} Supra note 148.

\textsuperscript{174} Adv. Tana Shpanitz, Deputy Attorney General, lecture at the Haifa Law & Tech. Workshop on New Copyright Legislation in Israel, Neve Ilan, December 11, 2002.

\textsuperscript{175} Ibid.

\textsuperscript{176} Birnhack, supra note 94 at 187.

\textsuperscript{177} Adv. Tana Shpanitz, Deputy Attorney General, lecture at the Haifa Law & Tech. Workshop on New Copyright Legislation in Israel, Neve Ilan, 11 December 2002.
level. In this position paper we deal with threats to privacy by the market, by those huge corporations becoming our "little brothers." The architecture of the digital environment makes it hard to regulate the conduct of such corporations, as they are "everywhere" on the web.\textsuperscript{178} Their activities are global.\textsuperscript{179} Therefore even perfect enforcement of the public regulation in a certain country will not eliminate the threats to privacy in that state. This consideration is particularly true with regard to states where the internal private threats to privacy are not substantial compared to the external threats. Where the public regulation is inefficient, it cannot be justified.\textsuperscript{180}

Moreover, when we deal with a sensitive area such as protection of privacy, we must take into account the limitations of legislation regulating privacy protection. Such legislation requires that the citizen whose privacy is violated sue the body responsible and thus expose his private matters to the public.\textsuperscript{181} In Israel court rulings are published on the Internet with the full names of the parties, therefore there is a fear of bringing action on sensitive matters. In addition, citizens whose privacy is violated are deterred from bring actions also because it is difficult to prove in court both the violation of privacy and the damage that it caused.\textsuperscript{182}

2. Private Regulation

Another option for dealing with the threats that the digital environment poses for the right to privacy is private regulation by the market forces: Internet Service Providers (ISPs), the content providers or even the users themselves.\textsuperscript{183} The market forces may

\textsuperscript{178} Lessig, \textit{supra} note 149, at 19.

\textsuperscript{179} On the difficulties in applying the law to a digital world without boundaries, see: David Johnson and David Post, "Law and Borders - The Rise of Law in Cyberspace", 48 \textit{Stan. L. Rev.} 1367 (1996).

\textsuperscript{180} Adv. Tana Shpanitz, Deputy Attorney General, lecture at the Haifa Law & Tech, Workshop on New Copyright Legislation in Israel, Neve Ilan, December 11, 2002.

\textsuperscript{181} Adv. Rivki Dvash, Consultation and Legislation Department at the Ministry of Justice, lecture at the Neve Ilan Workshop, December 17, 2003.

\textsuperscript{182} Ibid. In view of this problem, Adv. Dvash suggests awarding compensation without proof of damage. This is also suggested in the Bill of the PPA (Amendment no. 9) 2005. On the difficulties in estimating the damage see TA 7959/01 \textit{Segal v. Pharage} (unpublished) where the defendants made commercial use without permission of the plaintiffs' photo and argued that this publication did not cause real damage to the plaintiffs and that the PPA does not grant them compensation.

\textsuperscript{183} See the self regulation policy paper of the Israeli Internet Organization, \url{http://www.isoc.org.il/hasdara/hasdara_code.html}. 
lead to the formation of technological solutions, preventing violation of privacy,\textsuperscript{184} or to setting a privacy policy guaranteeing the protection of privacy,\textsuperscript{185} as well as to the creation of mechanisms to encourage surfing websites that guarantee the protection of privacy,\textsuperscript{186} and the formulation of ethical codes\textsuperscript{187} and education as well as the diffusion of social norms.\textsuperscript{188}

Private regulation has the advantage of keeping the Internet free from governmental intervention and of public control. In addition, it is assumed that market forces will lead to better solutions, unless there is a market failure that requires state

\textsuperscript{184} See for example encryption and digital signatures, Anonymizer, P3P (discussed below); e-mail filtering software, use of electronic tokens and changing internet technology in order to reduce the amount of spam (see Yaniv Drukman et al., \textit{Spam: Regulation of Unsolicited E-Mail} (Haifa Law & Technology Center, Niva Elkin-Koren and Michael Birnhack, eds., 2004).

\textsuperscript{185} In Israel it is not common for websites to adopt an appropriate privacy policy. A study conducted by Niva Elkin-Koren and Michael Birnhack, "Protection of Privacy on Public Websites" \textit{University of Haifa Journal} shows that only 8.1 of public websites in Israel that gather information on users display a clear privacy policy. About 70\% of the websites examined do not display a privacy policy and an additional 9\% display a policy that includes privacy protection, under a title that does not contain the word "privacy". In 0.9\% of websites the links to the privacy policy page are dead. It was found that those public sites that have a clear privacy policy do not meet the requirements of section 11 of the PPA about informing the user on the fact that information is gathered, the purposes and the uses of the information.

\textsuperscript{186} See e.g., TrustE used as a standard for sites, indicating that they meet requirement regarding privacy: \url{http://www.truste.org/}.

\textsuperscript{187} See e.g., the report of the committee on the Internet and Press Commission, which determined that the professional code of ethics should apply to Internet journalists: \url{http://www.law.co.il/computer-law/internet_ethics.doc}.

\textsuperscript{188} Dr. Naama Carmi considers that the Internet environment is human and ordinary standards of human conduct should apply (lecture at the Neve Ilan Conference, December 14, 2003), see for example the Treaty on Wise Use of the Internet (\url{http://www.amutat-eshnav.org.il/}), providing, among other things that:

*Privacy is a basic right constituting an essential condition for personal autonomy.*

- Technological means should not be exploited in order to violate the privacy of users in a manner that is prohibited in the "outside world".
- Personal data on user should not be gathered without their knowledge and the identity or other information on them should not be disclosed to third parties, on the Internet or otherwise, except as required under the PPA.
- Gathering and exposing information must be subject to informed consent: the users' right to receive accurate information on the data gathered about them, its uses, when their consent is needed and when the data must be given, and they may refuse to the gathering of information.
- Website owners and providers must have a transparency policy declaring the level of anonymity kept and under which conditions it can be removed.
- E-mail is considered "secret conversation" under the PPA and the Wiretapping Act, and it must be monitored except where the law provides otherwise.
- No unsolicited mail should be distributed without the explicit consent of the recipient and users must not be added to mailing lists without their consent.
- The e-mail addresses of mailing list members must not be disclosed to third parties.
intervention.\textsuperscript{189} Private regulation is also more flexible and has better tools for adapting itself to changing technologies, compared with public regulation. Therefore, private regulation will be the first step we will explore, in order to prevent a legal lacuna that would otherwise require legislative intervention.

The starting point is the assumption that the players in the virtual market prefer to design it by themselves, rather than have public regulation imposed on them.\textsuperscript{190} In order to avoid state regulation, these players have the incentive to design the digital environment in a way that serves not only their own interests, but also the needs of the general public.\textsuperscript{191} Therefore, they will be careful not to formulate rules which are incompatible with the general law.\textsuperscript{192} In addition, it can be assumed that the service providers will design rules that would please their customers, in order to create a respectable image to market their service.

Nevertheless, one must also acknowledge the disadvantages of private regulation, in order to balance the various means of regulation.

Firstly, \textit{there is a difficulty in privatizing the public discretion, i.e.,} in according private bodies with value-based decisions, which are not subject to constitutional or administrative law. Even if such arrangements lead to a desired result of the protection of the right to privacy, we cannot be sure that the balance of values made by the private entities was an appropriate one. Private bodies are motivated mostly by business considerations and these would most likely overpower the public interest, as long as the private bodies can maintain a level of conduct which prevents legislative intervention. In addition, private bodies suffer from a cultural bias. The Internet creates a complex system of connections between the "center", which creates the information, and the "periphery" that uses it.\textsuperscript{193} That center consists mostly of large American companies that can be assumed to act in accordance with the cultural standards familiar to them when formulating value-based arrangements, which may have a worldwide application.\textsuperscript{194} This point requires us to consider the question of whether we prefer to turn the world into a global village or to promote different

\textsuperscript{189} Birnhack, \textit{supra} note 143, at 426.
\textsuperscript{190} Birnhack, \textit{supra} note 94, at 186.
\textsuperscript{191} \textit{Ibid}, \textit{ibid}.
\textsuperscript{192} \textit{Ibid}, at 188.
\textsuperscript{193} Dr. Ribak, lecture at the Neve Ilan Conference, December 19, 2003.
\textsuperscript{194} Birnhack, \textit{supra} note 143, at 431.
arrangements in each state, according to its common moral and cultural standards. In fact, private regulation can lead to cultural control, reducing individual autonomy.\textsuperscript{195} A centralist power in the content market can influence the design of the information environment, as well as public preferences and current affairs.\textsuperscript{196} Such cultural control is especially problematic with regard to the right to privacy, which is subjective and cultural-dependent.\textsuperscript{197}

These difficulties are even greater since the interests according to which the private bodies operate, in many cases, are not transparent.\textsuperscript{198} The moral standard according to which the content market will be designed is not subject to judicial or public review, unlike direct public regulation.\textsuperscript{199} In fact, these bodies do not have to disclose their considerations and criteria at all. Therefore we have no real ability to consider the value balance between the private and public regulation on the basis of full information.

Secondly, in many cases, private regulation forms a limited tool, rather than an overall arrangement that would prevent the violation of privacy. There is a difficulty in enforcing private regulation. Private regulation is voluntary - the public cannot be forced to use it. In addition, when it comes to technological private regulation, it may be that only users who can afford it will enjoy it. We must ask ourselves whether we wish to live in a society where privacy is granted only to the rich. In such a society, the right to privacy can be used as a tool to increase the social divide.

3. Indirect Public Regulation

A third possibility for handling the violation of privacy on the web is indirect public regulation, granting legal incentives to the protection of privacy, without laying down provisions that determine what is prohibited and what is allowed. The role of the state


\textsuperscript{196} Ibid, ibid.

\textsuperscript{197} Supra notes 22, 23.

\textsuperscript{198} For example the criteria followed by filtering programs are not always known to their users.

\textsuperscript{199} Private regulation through contracts is an exception in this context, since once the contract is breached and the dispute reached the courts, it respects the freedom of contract but may not enforce it due to discriminatory term (section 4 of the Uniform Contracts Act 1982), or due to illegality or public policy (section 30 of the Contracts Act (General Part) 1973).
in this type of regulation is that of a player, who affects the results but does not dictate the rules of the game. Those bodies that are supposed to perform the private regulation through designing the architecture of the digital environment do not bear the cost if privacy violation, they are those who create it. The privacy violated is that of the citizens who do not participate in formulating the norm. Therefore sometimes the incentive to fill in the lacuna, so as to prevent legislative intervention, is insufficient.

In fact, indirect public regulation encourages, by legal means, private regulation of the digital environment. It changes the indicators used by private bodies to evaluate the profitability of their activities and causes the, to be compatible with the public interest.

An example of indirect public regulation is a law setting arrangements which are not binding, but create a presumption that whoever complies with them, acts in accordance with an appropriate standard of privacy protection. Another example is the amendment added to the Federal Trade Commission Act, authorizing the American Federal Trade Commission (FTC) to enforce privacy policies set by website owners voluntarily under the cause of misrepresentation.

Indirect public regulation has the advantage of not subjecting technology to law, unlike public regulation, but instead it tries to combine the two. In addition, since such regulation does not set binding provisions, the freedom typical to the digital environment is maintained. The market remains in the hands of the players rather than the state. The players may choose a course of action that grants them incentives or one that leaded to loses. However, indirect public regulation does not solve the main problem of privatizing the public discretion, granting it to private bodies that do not act in the public interest.

201 Lessig, supra note 149, at 159.
202 Ibid, ibid.
203 Birnack & Rowbottom, supra note 200, at 124.
204 An example of such an arrangement is the proposal of Adv. Dalit Dror, of the Israeli Ministry of Justice, to include a set privacy policy in the Law which will not be binding on websites, but will create a legal presumption whereby he sites that adopt it meet the requirements of privacy set by the state (lecture at the Neve Ilan Workshop, December 18, 2003).
206 On the activity of the FTC see http://www.ftc.gov/privacy/index.html.
B.6. Interim Summary

Our basic assumption is that we must not surrender to technology that enables new violations of privacy. The various possibilities for handling the threats to the right to privacy are public regulation (direct or indirect) and/or private regulation.

- **Direct Public Regulation** can be achieved through implementing the general law existing in the physical world to the digital environment, or through determining new legal rules. Its advantages are transparency, legal certainty and granting a moral approval to the protection of privacy. Its disadvantages are compromising the decentralized public discourse typical to the digital environment, an attempt to impose technology to the legal rules, an attempt that in many cases is bound to fail, and inefficiency on a global level.

- **Indirect Public Regulation** (legislation creating incentives, either positive or negative, but does not determine directly what is forbidden) gives legal incentives to private regulation. Such regulation does indeed resolve most of the disadvantages of public regulation, but the difficulties of privatizing the public discretion (see below).

- **Private Regulation** is achieved by market forces through technological solutions, privacy policies and contractual, through ethical codes or education and diffusion of social norms. Private regulation maintains the freedom typical of the digital environment, but is problematic since it privatizes the public discretion, granting it to private bodies having interests that are transparent, and since it is difficult to enforce.

With regard to any threat presented in this position paper we ask if it is appropriate to intervene and regulate this phenomenon. If we reach the conclusion that it is, we try to examine the appropriate means of interventions and its appropriate extent.
C. Consent

C.1. Introduction

Consent is required for almost any action taken in the digital environment. Consent has several meanings, which can be described as expanding circles, at the center of which is the consent to enter into a contract in its classic meaning, and in the outer circle, consent to virtual, intangible activity by the operators of the technology. We will describe four main circles of consent. From the most explicit consent, to consent to data processing. The further we move from the inner circle, the further we move from the field of contract law towards the issue of privacy on the Internet.

At the basic level, visiting a site constitutes some sort of consent, establishing some sort of a legal contractual relationship between the user and the site operator. This relationship can be recognized easily and the consent for its creation is given expressly by the user by way of behavior. Disputes that may arise at this stage are the closest in nature to regular contract law disputes.

On the second level is the consent to enter into online contracts for goods or services. In this situation the rules of the game change. These agreements are entered into in the virtual environment of the web. Although these are agreements in the classic sense of the word, the environment in which they are entered into creates new types of problems. Thus, for example, it is harder to identify the parties to the transaction, due to anonymity on the web and the technological ability to create an environment involving many participants (by linking sites, etc.). At the stage of the carrying out the transaction new problems arise, such as the inability to conduct real negotiations and the question of the essence of consent without real negotiations. Nevertheless, consent in these cases is normally obtained, at least on the formal level. In creating online agreements the requirement of explicit consent by the user appears often on the site itself (unlike the cases discussed below). The reason is that such consent is essential for the transaction and the site operator has an interest in requiring it in clearly.

On the third level, consent is requires in order to collect personal details. It

---

207 In this chapter we leave the discussion on consent on the web and discuss the element of consent to violation of privacy. However, it is important to note that a question arises also in the context of contractual consent on the web regarding its sincerity and validity in a modern contract. See for example Margaret Jane Radin, "Humans, Computers, and Binding" 75 Ind. L.J. 1125 (2000) where the issue of consent is discussed extensively as well as the problems arising from the new form of contracts, the absence of negotiation and the “take it or leave it” approach.
should be emphasized that these are not only details required in order to conduct a transaction, but any collection of details, whether or not they identify the person, collected for the purpose they were given or for a different purpose; given with intention of through lack of awareness. The question of consent in such cases is at the core of this sub-chapter.

On the fourth level, perhaps the one posing the greatest difficulties, both on the technical level and with regard to the question of the need for consent, is the consent to data processing. This is possible even after the user has left the scene. We should consider whether consent is required and what kind of consent?

The technologies in the digital environment allow for operation of functions in a one-sided manner by the operator, without the consent of the other party and without his knowledge. This is, inter alia, the novelty of the technological revolution. In the past, information given was kept in physical, tangible format, and therefore the ability to control it was essentially different. The assumption is that the architecture of the web will not allow the user to control the exposure of the information, at the first stage. Control of the use made of it later is more difficult and perhaps even impossible.

It should be noted that the answer to the question on the extent of consent to violation required on the web is not clear and far from being in consensus. Some argue that in the digital environment the users should assume that they are being monitored and therefore the concept of privacy should be adapted to the existing technology. This approach gives a wide interpretation to the concept of consent. Any consent, even the vaguest consent, should be considered valid. They see consent given by the user when entering the site, an act done voluntarily, as a sufficient base for consent. This type of implied consent or consent by behavior is recognized by the law (in the same way that boarding a bus constitutes consent to the agreement between the driver/bus operator and the passenger). On the other hand, others see the requirement for consent as the only way for presenting boundaries to invasion of privacy, boundaries that are vital for the quality of life we wish to maintain.

---

208 This approach was expressed by Dr. Yuval Karniel in his lecture at the Neve Ilan Conference. He argues that nowadays the need for privacy has decreased and people are interested in exposing themselves.

209 This approach was expressed by Adv. Haim Klugman, Chair of the Public Council for the Protection of Privacy and by Dr. Naama Carmi, in their lectures at the Neve Ilan Conference.
According to this approach, the requirement of consent is essential and should be construed narrowly by presenting a requirement of real consent, given in an express and informed manner.

Nevertheless, the common ground of these approaches is the basic need for consent. Those who give a wide interpretation to the element of consent do not argue that this element is unnecessary, and the differences revolve around the question of the extent of consent required and the level of awareness of the users to what exactly they give their consent, as the latter is derived from the former. We shall proceed from this starting point when we examine the subject: Consent is an essential element in data protection law. We begin with presenting the existing legal situation. Then we present data and empirical research on what is done in practice. We raise the problems and follow them with possible solutions.

C.2. The Existing Legal Arrangement

The Basic Law: Human Dignity and Liberty recognizes the right to privacy as a basic right. Section 7(b) of the Basic Law provides as follows: "There shall be no entry into the private premises of a person who has not consented thereto." This is the highest normative recognition of the right to privacy in Israel, and as a result, of the right to consent or not to consent to violations of privacy. This is the most general declaration establishing the existence of this right.

The Basic Law binds the State and its authorities. The extent of its application to private law is unclear. The approach of Supreme Court President Barak is that dignity and other enumerated rights are "supreme rights", spanning the law in general and should apply also to private law. But even if there is no direct application, this is a basic right, with everything that this status implies.

Two central laws deal with the concept of consent and are relevant to our discussion: The PPA and the Contracts Law (General Part) 1973.

Section 1 of the PPA provides as follows: "No person shall violate the privacy of another person without his consent." The Act lists several cases of violation of privacy, but the privacy is left undefined and remains vague. Without clear boundaries

210 On applying public law norms to private law see TA (Tel Aviv) 15/97 Batia Shamsonian v. GaniRozmari Restaurant, 14 Dinim Shalom, 402; TA (Jerusalem) 11258/93 Avraham Naamne v. Kibbutz Kalia, 6 Dinim Shalom, 236; HCJ 721/94 El-AL Israeli Airline v. Daneilovitz, 48(5) P.D. 749.

211 See chapter 1.A above.
the protection of the right to privacy is unclear too. It is impossible to know when and
to what extent consent is required. The more we widen the boundaries of the right to
privacy and with them its protection, the stronger the requirement for express consent
will become. Beyond the declarative aspect of the above provision it does not provide
any information on the acts required in order to obtain consent and protect the right to
privacy. Section 3 of the PPA defines consent as "explicit or implied". This definition
fails to clarify the piratical requirements. An "implied consent" could also be the act
of surfing itself, as an implied consent to any online activity. It is unclear which wide
interpretation can be adopted under the said definition.

Section 2(9) of that PPA provides that violation of privacy is "use of
information pertaining to one's private matters or its transfer to others for a purpose
different than the one for which it was provided." This appears to apply to all of those
cases where details are gathered and kept, when provided by the user for a certain
purpose and used for some commercial purpose. For example, the Hevre\textsuperscript{212} web site
requires the user to provide personal details in order to locate his or her friends and
publish his or her own details. These are then used by the site operators as a classified
database, sold to e-mail advertisers.\textsuperscript{213} Prima facie, the details were provided for a
different purpose than that for which they are used in practice. Thus, it seems that
privacy is violated under section 2(9) of the Act. However under the PPA, if the
information was provided with consent, including implied consent, this does not
constitute violation of privacy. This case demonstrates the claim that the ability to
enforce this provision is negligible. The ability to control information exists at the
stage when it is provided. Technological developments prevent supervision and
enforcement of the unlawful use made of the information. This issue will be
demonstrated below through empirical research on privacy on the web.\textsuperscript{214}

Another relevant legal arrangement is based on contract law, providing that
decisiveness by both parties is required in order to enter a contract.\textsuperscript{215} In the words of
Professor Gabriella Shalev: "Decisiveness is an established will, a serious intent to
enter the contract and decisiveness. Unlike intention to create legal relations, which is

\textsuperscript{212} \url{http://www.hevre.co.il}.

\textsuperscript{213} According to Mr. Shlomi Unger, CEO of Mahshava, the operator of the Hevre site at the Neve Ilan
Conference.

\textsuperscript{214} Supra note 184.

\textsuperscript{215} Contracts Law (General Part) 1973, sections 2, 5.
abstract and general, decisiveness must be defined and aimed at a particular contract with a particular party...  

Decisiveness has its external expression in the consent of the offeree, whether by behavior or in writing. Naturally, the more express and clear the consent, the better evidence it is of decisiveness (although it has been held that signature is not sufficient evidence of decisiveness). The less express the consent, the harder it becomes to find out whether there was decisiveness. As already noted, in the digital environment, the mere existence of consent does not necessarily indicate decisiveness and the question on the essence of consent remains an open one.

The principle of consent has also been discussed in an interim report issued by the Ministry of Justice on the subject of electronic commerce. Some of its authors chose to not to define the issue of consent, and the committee recommended that:

"The committee has reached the conclusion that there is no room for making the execution of contracts by electronic means conditional upon the consent of the parties (or absence of objection by them). Such a condition alters the general contract laws and should be specifically required only where one party drafts the terms of the contract."

With regard to contracts where one party drafts the terms of the contract, the committee suggests that the party who drafts the contract allow the other party to read it before entering into the contract, without prejudice to the uniform contract laws.

We saw that there is a legal arrangement with regard to the issue of consent only from the contractual aspect and the aspect of privacy violations. Yet beyond the vagueness of this arrangement and the ability to stretch it to the extent it becomes void, it cannot be enforced in the digital environment. This is an arrangement enacted prior to the digital environment; therefore it is not adapted to the new legal reality created as a result of it. Even if we enforce it and require real decisiveness for every action that requires consent on the Internet, this will hinder the operation of the entire system (and perhaps even paralyze it), make surfing harder and compromise the efficiency of the technological tool. The data brought below demonstrate the large gap

219 *Ibid*, at 27.
between the law in the books and the law in practice.

C.3. **Privacy on the Internet in the Practical World**

Two empirical studies are presented below. The first deals with the extent of obedience of website operators to the PPA (hereinafter: Privacy on the Internet),\(^{220}\) and the other deals with the level of awareness of users and the extent of their willingness to disclose information (hereinafter: the Awareness of Users).\(^{221}\) These two perspectives easily display the full picture and enable us to gain in depth understanding of the extent of the problem created on the web. This problem grows ever greater in light of the enormous quantity of personal information transmitted online and the ignorance of the consumer about information leaks and perhaps even intentional unawareness ("hiding your head in the sand").

The study on Privacy on the Internet examined active Israeli sites operated by public bodies. The findings of the study show that the extent of compliance with the law is very low and mostly non-existent. At least 50% of the sites examined gathered some kind of information on the users,\(^{222}\) beyond their name and contact details, and are therefore under the duties imposed on "databases."\(^{223}\) Among the legal requirements examined, there were few sites that followed the provisions of the duty to inform users whether there is a legal duty to submit the information (3%), the purpose for which the data is collected (15%) and to whom they may be transferred (5%).\(^{224}\) None of the sites examined mentioned the right to access the data gathered or the right to correct inaccurate data.\(^{225}\)

In view of the conduct of the sites, it is worrying to discover the low level of awareness among users. The study on the Awareness of Users examined Israeli users who have an Internet connection at home. It was found that only 31% of the users assume that even if they do not give personal data, the site keeps a record of data

\(^{220}\) *Supra* note 184.


\(^{222}\) This study was limited to the differences between the law and the sites’ declarations. A further research examined the differences between the declarations and the practice.

\(^{223}\) Chapter B of the PPA.

\(^{224}\) Section 11, *Ibid*.

\(^{225}\) Section 14, *Ibid*.
about them.

This finding expresses the low level of awareness among users about violations of privacy on the Internet. The percentage of Israelis who consent to disclose information is no more than 40%. At the same time, 71% of Israeli users believe that they ought to have the legal right to know anything that a website knows about them. These findings show support for the approach of keeping the boundaries if privacy invasion.

Another finding discovered in this research was that only 37% of Israeli users claimed that the fear of the possibility that a stranger may discover information about them has grown since they started using the Internet. This finding is particularly interesting in comparison to the 60% of American users who claim the same. It is likely that the difference in the level of awareness inherently leads to a difference in the level of fear. Therefore the percentage of Israelis aware of the possibility of gathering information about them without their knowledge and consent is close to the percentage of Israelis whose fear has grown since they started using the Internet.

This leads us to the conclusion that the existing legal arrangement does not protect the users and it does not protect the "weaker" population in this context, the users who lack awareness and whose privacy is violated more often.

We ought to add that online anonymity may create an illusion of privacy. Often anonymity is confused with privacy. The fact that the user cannot be identified does not necessarily lead to the conclusion that his privacy is protected. The amount of data that can be gathered without any cooperation by the user, about him or her and his or her consumer conduct, is enormous.

The existing legal arrangement is incompatible with the new reality and does not provide efficient solutions to the new legal problems. In our opinion the main problem with regard to the element of consent is the lack of information: the ignorance of the user about the details gathered about her without her knowledge and consent. Narrowing the gap may lead to a solution, since the market conditions will cause website operators to compete by minimizing the data they collect. They will have an interest in minimizing the violation of privacy.

As already noted, section 11 of the PPA could, if it were implemented and enforced, regulate the problem of lack of information to some extent. The said section requires the owner of a database to inform users about the legal duty to provide information, the purpose for which the data is gathered and the bodies to which they
can be transferred. This arrangement is hard to enforce, as it does not specify where
the notice should be published and a site can publish these on a page that the user may
find hard to reach. In the Privacy on the Internet study, the extent to which the privacy
policies are highlighted and accessibly was also examined. Low marks were given in
the evaluation of whether the pages were highlighted (3.49/5 on a 1-5 scale; 5 = not
highlighted. The standard deviation was 1.1) and similarly in relation to accessibility
(3.48/5, standard deviation 0.98). In the absence of such a definition there is a "double
lacuna" - both die to the technical ability of the user o reach the information, and the
difficulty in following implementation and enforcing the law. Therefore a new legal
arrangement should be formulated, adapted to the new reality in the digital
environment.

C.4. Private or Public Regulation?

Our assumption is that the main problem in relation to the element of consent in the
digital environment is lack of information about the problem. A special arrangement
should be formulated in order to prevent one-sided exploitation by the parties holding
power and knowledge. It should be stressed that there is a gap between the user and
the web site operator both in terms of knowledge and in terms of technology.

1. Full Public Regulation - Why Not?

There are cases where information gaps have led to full public regulation, for example
on health issues such as smoking or AIDS. The fear of lack of awareness about the
damages caused by smoking or unprotected sexual intercourse, led the state to
intervene. Such intervention is done through intensive advertising in the press and on
TV and by imposing a duty to state on every pack of cigarettes that "smoking is a
health hazard," and the like messages. Informing the public in such a way by the
state is irrelevant in our case. The main reason is that the cost of the lack of
information (which often led to diseases) was born by the state. This is not the case
here, when we discuss violation of rights and even if we could estimate it, we are

\[ \text{http://www.privacyalliance.org/}\]

\[ \text{Section 9 of the Restrictions on Tobacco Advertising Law 1983.} \]
dealing with the private market and the cost is born by the user or the site operator.

2. Full Private Regulation - Why Not?
We could "give up" and accept the fact that the many advantages gained through the technological developments involve waiving the right to privacy. The law does not intervene with the technology markets, not even by indirect intervention. Such an approach lead to privacy protection only for the rich, as the technological race is characterized by a dialog: software used for surveillance is exposed by software designed to find them.\(^\text{228}\) One development follows another and the law cannot respond to this situation; the ability to handle this is in the hands of the rich only - those who can keep up to date and purchase the most expensive protection of their privacy. The perception of our legal system tries to avoid such inequality; therefore we may assume that such an arrangement will not be welcome.

The conclusion is that the possible solutions lie between these two ends. Our assumption is that we are now in an interim period requiring unique solutions. With time, the implications of the Internet world on our lives will become clearer and the awareness about the risks of violations will grow. In such a state of affairs, the market failure created by the lack of information will be solved, at least in part. Due to the lack of information the market forces cannot bring about the most efficient economic solution, and certainly not a fair one. It appears that at least during the interim period, the legislator has the duty to regulate this issue and it should not be left to the market forces. The regulation we need to formulate should begin with legislation (namely, public regulation) and continue with the free market (private regulation). All we need to do now is "start" the system and cause the market to act more efficiently.

Below we suggest possible solutions, and focus on one model. It should be stressed that any solution has limitations and problems and we do not propose to create a perfect solution. Yet we believe that they may improve the legal situation and regulate in the most efficient manner the boundaries of privacy invasion in a world of developing technology.

\(^\text{228}\) See the chapter on means of surveillance.
C.5. Possible Solutions

Before we discuss the possible solutions in detail, we offer a re-examination of the types of information on the Internet. We submit that the distinction between personal information and information including name, address and contact details is less relevant in the digital environment.\(^{229}\) *It is more appropriate to draw a distinction between personally identifiable and non-personally identifiable information.* There are two reasons for this distinction: first, it is likely that gathering personally identifiable information requires some co-operation by the user. Therefore the ways in which we handle the problems raised in this context are different than in a situation where things are done without the knowledge of the user. Again, we are discussing the gathering of information and not the use made of it at a alter point (data processing, data mining etc.). Secondly, non-identifiable information serves economic purposes (mostly advertising or market analysis), and yet it violates privacy to a lesser extent. When we strike a balance between the violation of privacy and other interests, in his case - economic interest, the fact that the violation of privacy is relatively weak can create a balance that may justify it under certain circumstances.

A similar distinction is used in the U.S. Section 22 of the Telecommunication Act of 1996,\(^{230}\) defines and regulates the protection Consumer Proprietary Network Information (CPNI).\(^{231}\) The section divides the information about the client into three categories. The first and second categories deal with general information about the client and his habits, and are mostly used for internal purposes of communication companies, but the information can be sold to third parties. The client need not be informed in advance of such information and his consent is not required. However, the third category includes information that identifies the user in a specific way. Gathering, keeping and using such information is prohibited, save for information needed for the system operation and for collecting payments. For this purpose, the client's approval is required. Yet it should be noted that this section has been criticized. First, should the approval be an "opt-in" or "opt-out" approval? Secondly, what is a communications company? And thirdly, and most importantly, the constitutional freedom of speech is infringed. This lack of clarity led various

---

\(^{229}\) Section 7 of the PPA defined a database and excludes a collection including only names and contact details.

\(^{230}\) Telecommunication Act 1996

\(^{231}\) The Act defined the CPNI in section (h).
companies and other bodies to address the Federal Communication Commission (FCC) in order for it to lay down clear definitions. Indeed, it was held that the provider can gather and process data and use it for marketing purposes only within the framework of service provided to the consumer. The information on the client cannot be used for any other marketing purposes that the client has not subscribed to, unless he gives his express consent in advance (opt-in). Appeals and reservations have been submitted with regard to these regulations. The US WEST Corporation argues that these regulations violate the first amendment on the freedom of speech - the right of the provider to provide marketing offers to the consumer. Therefore they considered that the opt-out approach should be adopted, instead of the opt-in approach. The court accepted this appeal and held that the regulations do violate the first amendment and that the opt-in approach should not be adopted.

A. Technological Model
Can "The machine be the answer to the machine"? We refer to the technological model that can represent the will of the user: Privacy Enhancing Technologies (PETs). For example, the P3P technological standard enables the users to choose the level of privacy they are interested in and accordingly surf sites with that privacy level, or higher. However, this system has several advantages:

1. It maintains the technological efficiency of the Internal, because compared to other arrangements this arrangement does not hinder or paralyze surfing.

2. The system creates a competitive market, competing for "minimizing information" and maintaining privacy. Site operators will use only the minimal information they need to gather for their own purposes, in order to maximize the number of potential users.

3. This is private regulation. The advantage of private regulation is non intervention by the state which can cause the market to produce the most efficient solution. However, this advantage assumes that there is a maximal amount of information available. This assumption can only be true if the user rates the level of privacy and he therefore must be aware of it. It may be that this assumption is not realistic.

The disadvantages of this system are:

1. A scale of privacy must be set by a responsible, objective party. The question is - who should set the standards and levels of privacy? ("who will guard the guards") on what criteria should the sites be rated? Who will supervise?

2. The information problem remains, this time in the sense of information overload. In order for the average user to be able to make a real choice of privacy level, the user must know the meaning of each of them. This creates fear of information overload. The average user may become indifferent to the information, due to the large amount of information.

**B. Contractual Arrangements**

Can the contract law provide an appropriate answer?

(1) Section 4 of the Uniform Contracts Act of 1982 (UCA) lists the circumstances in which there is a presumption of no consent. The presumption can be rebutted. The purpose of the UCA is to protect consumers where there are no prior negotiations before the contract is signed. It is possible to create a legal arrangement, whereby there is a presumption of no consent by the user for gathering personal information. In fact, this can be achieved by imposing an "opt-in" system and ruling out the "opt-out" system. 233

The advantages are:

1. It is easy to enforce. In this case the interest in giving the information and presenting the opt-in possibilities is that of the site itself and therefore it can be assumed that the information will not be presented on hidden pages and it would be easier to follow the implementation of the Act.

2. It will increase the chances of obtaining real consent. The requirement to check "I am interested in disclosing information/receiving information from the site" and the like, requires a higher level of awareness than the requirement not to change anything. The mere act can raise awareness.

The disadvantages are:

1. Severe infringement of the freedom of speech and freedom of vocation of the site operator. We must remember that against the right to privacy and autonomy stand other rights owned by the site operators. In this case, it may be that a presumption of

233 Supra note 219.
no consent violates the appropriate balance between the protected rights.

2. An economic disadvantage. It may be that such intervention in the market will lead to a loss of economic opportunities. Some users are indifferent to the possibility of giving information and do not trust the "opt-in" option, and thus business opportunities may be missed.

(2) Section 24c of the Consumer Protection Act of 1981 regulates distant sales transactions. The Act imposes a minimal duty of disclosure in distant marketing: the name and address of the trader in Israel and in other countries; the main characteristics of the goods or the service; the price of the goods or the service and the options for payment; the time and means of supply; the period during which the offer remains valid; other details about warranty for the goods; the consumer's right to cancel the contract in accordance with the provisions of subsection (c). In addition, the trader must provide the consumer with a written document, including, among other things, the way in which the consumer can cancel the transaction; information in the warranty and other conditions.

We should consider the implementation of this arrangement on transactions on the web. In distant sales transaction, like online transactions, there is a gap between the consumer and the business. The intervention of the law has the objective of narrowing down this gap. It is caused in part due to the inability to see the goods or conduct real negotiations. As already noted, these problems are raised in the context of online agreements.

C. Informed Consent - Creating a Model

This model is explained in length. We go outside the existing legal framework (Contract Law and existing PPAs). This model has an element of novelty in the legal perception of the digital environment, as it adopts a model from a completely different field. At the time this position paper was edited, the Ministry of Justice issued a memorandum proposing an amendment to the Law so as to include an express definition of "Informed Consent", which is now part of the Bill submitted to the Knesset:

"Informed consent: consent received after the information reasonably required in order to decide whether to consent to a violation of privacy, given in an
understandable manner for a reasonable person.\textsuperscript{234}

The explanatory notes stress the need for such consent especially in the digital environment: "the need to clarify that the consent must be informed has grown in the Internet age, when waivers are often hidden from those whose privacy is violated."\textsuperscript{235}

In order to give meaning to this concept, we seek to examine the medical model of informed consent. The reason for using this concept is the wish to narrow down the gap between the users and operators. As already mentioned, these are gaps in information and in technological ability. The base for this model is passing the burden of responsibility for giving information to those in power, although the system is contractual. It is clear to us that there is a substantial difference between the two fields and we do not propose that the model be copied in its entirety, or that there is justification for doing so. However, the grounds for creating the legal arrangement of informed consent in medical law are mostly similar to the grounds for intervention and regulation of consent on the web. This similarity led us to the conclusion that a special model should be created for consent on the web, in the same way it was created in the medical field. The similar justification should at least lead to the recognition that there is no other way than to create a new arrangement, adapted to the new reality in which we live today and that in the absence of such an arrangement, the rights of the user are severely violated.

Our preliminary argument is as follows: in order to provide appropriate protection to the right to privacy, we must set standards in the digital environment. The main reason is that any other arrangement cannot be enforced.

Consent on the Web vs. Informed Consent in Medical Law

(1) What is Informed Consent?

The concept of informed consent is not foreign to the law. Thus, for example section 13 of the Patient's Rights Act of 1996 deals with the requirement of "informed consent" to medical treatment. The requirement of informed consent requires the physician to give the patient comprehensive information on every medical treatment suggested to him, in order to receive his consent. There are two elements in this concept: consent and receiving information. Consent must be free, without coercion

\textsuperscript{234} The Bill of the PPA (Amendment no. 9) 2005.

\textsuperscript{235} Ibid.
and based on full, clear information.²³⁶  

(2) Informed Consent as the Right to Autonomy  

Moral philosophy defined four elements of the autonomous act: fitness, intent, understanding and free will.²³⁷ The last two elements are the most important ones for the current discussion. Giving information is insufficient. It must be verified that the party receiving the information is capable of understanding it. The right to autonomy has been recognized as a basic right under Israeli law. In the words of former Supreme Court President Meir Shamgar in the case of Noam v. Dr. Weigl:²³⁸ "The case law dealing with the requirement that the consent of a patient to medical treatment is informed, the standard of disclosure required of a physician as set while taking into consideration, first and foremost the basic right to autonomy. Therefore it was held that the physician must be informed of all the risks that a reasonable person would consider important in deciding whether to consent to the treatment. The element of free will has also been recognized under Israeli law as a basic right, even in circumstances of pressure and dependency."²³⁹  

(3) The Justifications for the Requirement of Informed Consent  

The process of giving information and the requirement of consent naturally create trust and respect, but there are stronger considerations that led the legal system to create the strict requirement of informed consent in the medical field.  

* Differences in power: Moving from the paternalist model, where all decisions are made by the physicians only, to a collaborative model.²⁴⁰ This involves the recognition that the wished and needs of the patient should be taken into consideration. This principle reflects the understanding that the physician has professional knowledge that the patient does not have, and there is a fear that due to these divides, the physician may have the exclusive right to make decisions about the body and life of the patient. It is clear that the differences cannot be bridged and the physician still has broader knowledge than that of the average patient. Yet the arrangement requires the physician to share the relevant information and thus taking  

²³⁷ T.L. Beauchamp & J.F. Childress, Principles of Biomedical Ethics (3rd ed.) 69.  
²³⁸ CA 3108/91 Raivy Noam v Dr. Kurt Veigel, 48(5) P.D. 497, 509.  
²³⁹ Supra note 30 at 18.  
the exclusive decision making power out of the hands of the physician.

In the digital environment there are differences in knowledge and technological ability between the user and the operator. It can be argued that these can be narrowed down easily by users learning about these issues, as the information is accessible (unlike medical information requiring years of studies and experience). However, these days, any type of information is accessible, including medical information and yet the differences are maintained. Hence the justification remains valid. Even if we could assume that the average user has sufficient knowledge about the digital environment, the technological race renders any information that the user has irrelevant. The difference in technological abilities is also maintained, especially due to economic inequality. The average user's ability to face the technological abilities of the operator is minimal. The greater the differences, the more essential it is to strike a balance between the parties and bridge the gap as far as possible. *Standardization in giving information by the site about the details gathered and their uses will narrow the gap to some extent and enable the user to decide out of his or her own free will whether to allow personal information to be gathered or not.*

The process allows for choice of a different treatment: giving data allows the patient to choose his preferred treatment. The decision is taken out of the hands of the physicians and given to the patients. This justification can also be used in relation to the matter at hand. The wide array of options on the Internet can allow the user to choose a site that takes the smallest amount of information from him. Clearly, he must know what data is collected, by imposing a duty to give information on the details collected. This will create better market conditions for competition on "minimizing the information collected", which is desirable when it comes to protection of privacy.

Waiving treatment in cases of serious risks: It is recognized that the patient has the right to waive treatment. By analogy one could argue that once the extent of privacy violation is published, the user will be able to waive the specific act he wished to perform or the use of the Internet. For example, if the user knows that purchasing a product on a certain site will involve exposing information that he does not wish to expose, he may choose to purchase it in a different way. This would also force the sites to compete or "minimizing information."

---

241 CA 4384/90 *Shimon Vathori v. Leniado Hospital*, 51(2) P.D. 171.
242 *Supra* note 238.
Giving up surfing altogether is undesirable and is unlikely to be encouraged, mainly because of the substantial progress achieved due to the influence of the Internet on our lives. But realistically, it is clear the use of the Internet will not stop mainly because of its efficiency, and yet the collection of information will be minimized and there will be no reason to give up surfing altogether. Over all, it is important to note that the right to give up use is derived from autonomy and must also be enabled.

We ought to add that the advantage of standardization of the digital system is even stronger than that of the medical system, with regard to encouraging the market. While every physician is naturally motivated to minimize the risk to the patients, site operators do not have any motivation to minimize the information collected, and only through public regulation can such motivation be manufactured. Furthermore, today information has a high economic value and in the absence of sanctions and defined borders, the motivation is to maximize the information collected.

A Solution and its Implications
We support the proposition of the Ministry of Justice to add a requirement of informed consent in regard to data collection in the digital environment. Can this be broken down into particular duties, or should it be left as a standard, to be formulated by the courts on the basis of accumulating experience? The latter option will leave a greater array of action for site operators, the extent of intervention in their right to run their site as they wish (a right that has aspects of freedom of speech, freedom of vocation and the right to private property) will be smaller and proportionate. We prefer this solution to a requirement of giving details on how the information should be given (such as a duty to publish the information on a specific page on the site, highlighted in a particular way, etc.). However, a general model can be suggested, to make it easier for site owners and users and to lower the costs for the site owners.

C. 6. Interim Summary
Our review shows that the attempt to settle for the existing legal arrangements is bound to fail. In practice, the law is incompatible with the new reality and in any case it is not fully implemented. The model we focused on is that of giving information and creating uniformity. We borrowed the notion of informed consent from the field of medical law. Despite the difference between bodily injuries and privacy violations,
some interests worthy of protection are common the two fields. Among them free will and autonomy, that have been long recognized as basic rights. Beyond these, it should be recognized and realized that the existing state of affairs is problematic and enables the violation of rights. The same considerations that led the legal system to intervene with the relationship between a physician and a patient are also valid in intervening in the relationships between a user and an operator.

The existing legislation establishes the principle of consent in the legal world, but is insufficient and is incompatible with technological progress. A new solution must be found for the new situation and the many difficulties in enforcing the law in a virtual environment. A partial solution, in the absence of a better alternative, can also improve the legal situation. The fear of the unique problems of the digital environment is real, but this does not, in our opinion, justify standing still and creating a lacuna that enables the violation of privacy which is a basic right under Israeli law.
2. Digital Means of Surveillance

A. Introduction

The digital environment has an architecture that enables gathering data during the communications between computers connected to the network. Sometime gathering data is a byproduct of another application and sometimes it has the purpose of surveillance. The data gathered is stored in databases, on which we elaborate in the following chapter. In this chapter we review the main means of surveillance in use these days and evaluate the ability of the technology. The review is aimed at establishing an understanding in relation to violation of privacy and to enable us to formulate informed solutions, whether legal or technological (or a combination). The means of surveillance can be classified in several ways. We shall focus on the classifications we consider the most important, in accordance with their purpose: are they a byproduct of the architecture of the web or are they intentionally aimed at gathering information? We draw a distinction between two groups:

(1) Means of surveillance with the sole purpose of surveillance, for various uses. These include web bugs, Trojan horses, spyware and private applications created by crackers- hackers. These collect as much information as possible on strategic targets of their operators, such as the system administrator password on the user's PC and password of virtual bank accounts, bank account numbers, credit card numbers, contents of messages sent through e-mail, the identity of chat or forums participants and so on. The arsenal of activities used by these means of surveillance is varied, and may include distant control of the PC or connecting via Telnet to one computer and through it to other computers.

(2) Means of surveillance with other uses which are not marginal, alongside their function of monitoring activities and pieces of information on the web. These include cookies, sniffers and of course, cellular phones.

There are two main methods of internet connection: an analog modem and broadband connection (ADSL and cable modem). Statistically, an average computer with a broadband Internet connection is scanned by different parties at lease 12 times.

---

243 Other possible classifications: the physical place of activity of the means of surveillance - some are located in the physical layer of the web (sniffers) and some break into the computer systems themselves, whether personal or organizational (cookies, web bugs, spyware and Trojan horses).
a day, in order to find loopholes or in attempt to invade it.\textsuperscript{244} Those with standard modem connection, who initiate the connection only while surfing are not immune from such attempts, since most ISPs use the Password Authentication Protocol (PAP) that does not encode the name and password of the user.\textsuperscript{245} The first part of this chapter examines the various technological means through which data can be gathered and the other part examines different types of solutions, legal and technological and evaluates their potential.

B. An Examination of the Various Aspects of Digital Means of Surveillance

In this part we review in depth the digital means of surveillance. Since there are different types of means of surveillance with different functions and posing different threats to privacy, we chose to focus in this chapter on each type separately, while explaining the method of action, the technology, the aims and the problems it raises in relation to privacy. It is important to remember that the means of surveillance are part of the larger internet network and as such are influenced by its structure and functions, and exploit them. Therefore we begin with a general explanation of this structure. This explanation presents essential basic concepts and gives a certain view of the way in which the web operates.

B.1. The Architecture of the Web

The concept of the "web" is derived from the unique architecture of this communication network, allowing computers in different places to connect to each other. Visually, it resembles cobweb, as opposed to a hierarchical structure where one computer controls all others or a linear connection between two computers only. The Internet began with a project of the U.S. army in the late 1960s, aimed at creating a technology that enables computers on the network to communicate even when the connection between them is interrupted.\textsuperscript{246} The system developed was Packet Switching, a system for transferring information by dividing it into packets, including,

\begin{itemize}
  \item Avi Weiss, "Knowing the Danger", YNET, 23 April 2002, \url{http://www.marketing.co.il/magazine/2002/18/Ynet.htm}, last visit on March 24, 2005.
  \item Ibid. It should be noted that the only exceptions in Israel are ISPs Bezeq International and Barak that use the CHAP (challenge handshake authentication protocol) which encodes the username and password.
\end{itemize}
other than the pieces of information, also the address of the sender, the computer to which it is sent and a serial number that enables recompiling the packets of information. The packets of information sent reach the closest computer on the network; it reads the addresses and transmits them forward to the destination, so that in case of malfunction, it is possible to find alternative ways to transmit the information. The flow of information resembles mail sent across the country - from the sender to the post office, that delivers it to the city of destination and then to the neighborhood and to the mailbox of the recipient. The Internet is a machine taking packets of information created on the web and transferring them to their destination. The transfer involves different back stage mechanisms. Following is an explanation of basic web terminology.

**Protocols:** The language used for communications between computers on the Internet. The protocols determine all the details about the ways of communications between devices (hardware and software). There are millions of protocols for performing an array of tasks. The most basic ones control the way in which the Internet operates, namely they control the patterns of the pieces of information and the way they are transmitted between computers. This basic protocol is the Network Protocol, also known as Internet Protocol (IP).

The way in which the information is divided and compiled is determined by higher level protocols. The Transport Protocol controls the transmission from one place to another. There are two common types of Transport Protocols, in accordance with the type of information transmitted. E-mail and files are normally sent through a TCP/IP (Transmission Control Protocol), optimal for effective transmission of information packets without errors. Media such as video or audio uses UDP (Use Datagram Protocol) that enables control over the transmission and receipt of the information packets on after the other. The Application Protocol renders the received transmission into something recognizable by presenting it as an application.

**Client/Server Model:** One program (the client) requests a service from another program (the server). An example of a common use is reading e-mail through

---

250 *Ibid, ibid.*
software such as Outlook Express or Eudora. The software is the mail client and the computer from which the e-mail is downloaded runs a program called a mail server. This model requires the client computer to find the server computer. This is done through Internet addresses.

**Internet addresses:** In order for a computer to be able to communicate with another computer, there must be a way to identify the computers. Identification based on the physical location of each computer is as ineffective as a mailbox address, since the computers can connect to the network from different arbitrary places. On the Internet each computer has a unique address, the server addresses are permanent and the client address may be permanent or not.

In order to understand the operation, we describe a process of finding the address of a website. Whatever type of Internet connection is used, it is always essential to have someone on the other side to direct the pieces of information to other computers on the network. This side is the Internet Service Provider. To which the client computer is connected.\(^\text{251}\) Once connected, the client computer receives an IP address, which includes an identifying number of the network in which the server operates and a number unique to the computer. When we, as users, type the address of the website using letters, this is done for our convenience, because as humans it is easier for us to remember words rather than numbers, but the address is then translated into an IP address by the Domain Name Server (DNS).\(^\text{252}\) This system turns domain names into IP addresses understandable by computers. You may think of it as a phone book containing a list of computers and their IP addresses. After the translation the client computer knows the server address and can approach it to request exchange of information. In such a request the client computer specifies its address, so that the information sent can reach its destination, and a connection is created between these two IP addresses.

The fact that every computer has a unique IP address has implications. In terms of anonymity, any computer on the web has a unique IP address, that makes it possible to identify the server through which it is connected and through that server - the individual user. The identification of the server and the country of origin can be done through the IP address. The identification of the individual user is information found


\(^{252}\) Ibid, at 25.
on the records of the ISP and its disclosure is subject to the law and to the ISP's policy. It may require cross processing of data from several databases, but it is possible.

In terms of privacy, a distinction should be made between a permanent Internet connection, where the computer has a permanent address, which makes it possible to collect information and cross process it while linking it to a specific user and between a connection where the IP address changes, in which case the violation of privacy is not as severe, since it is limited to one's use that makes it more difficult to follow a user over a long period of time.

a. **Cookies**

Cookies are currently an integral part of Internet browsers. Many users do not know of their existence and are unaware of the threat they pose to their privacy. In this part we attempt to shed some light on this common means of surveillance. The cookies operate in a similar way to a cleaning service: the user hands over his laundry and gets a receipt. When he returns to pick up the clothes, the receipt he presents is used in order to know which clothes belong to him. Without the receipt, there is no way of knowing which clothes belong to which client and whether the client is a new one.

Online cookies serve a similar function. Every visit and every action on a website - the site cannot tell whether the user is new or old and the cookie serves as a means for identification, in order to identify and trace the visitors. Cookies were developed in the early 1990s by Netscape Communications Corporation. The term "cookie" derives from "fortune cookie", in programming language, a piece of information common to several parts of the software acting in collaboration. The purpose of developing cookies was to enable the server to follow the requests by the user. This is required in complex sites where the connection between the different pages should be kept.

Cookies are text files containing information and saved to the hard drive of the user. In general cookies are created by the web page server, which is the computer through which a site operates. The information kept in the cookies is created by the server when a user visits a site and can be used by the same site in future.

---


Therefore some consider the cookie a "user ID" for a specific site, informing the server that the user is visiting again. This is what a typical cookie looks like:

```
HMP1 hotmail.msn.com/ 0 1715191808 3210782
1236821008 29449527 *
```

First the cookie is saved to the user's hard drive (without his knowledge or consent) and it includes several parameters created by the server, which are in fact a string of the user's preferences. The browser reads the cookie and saves it in a special file.

Then the browser automatically sends the cookie with every request from the site. Every time the user visits the site, the browser sends the cookie containing the personal information on his preferences to the site server, without his approval. The information contained in the cookie is not only the username, but there are at least six parameters that can be transmitted:

a. The name of the cookie - mandatory
b. The value of the cookie - mandatory

c. The expiration date of the cookie

| The date on which the cookie expires and is to be deleted from the system. If no date is specified, the cookie will be deleted when the session ends. In some cases the default time is 20 minutes. |

The date structure: DAY, DD-MMM-YYY HH:MM:SS GMT

DAY- the day of the week
DD - the date of the month (01, 02…)
MMM- a three letter abbreviation of the name of the month (Jan, Feb….)
YYYY - the years
HH - hours (10:00 = 22:00)
MM - minutes

---


256 The name of the file depends on the type of browser used. These files are known as "cookie jars". Garfinkel, supra note 254, at 221.

257 [http://www2.eitan.ac.il/cookies/ProffIntroduction.asp](http://www2.eitan.ac.il/cookies/ProffIntroduction.asp), last visited on March 24, 2005.

258 It should be noted that this date format appears after translated by Java. The cookie presents a TimeStamp - the seconds that passed since 1 January 1970.
SS - seconds
The cookie can be deleted by specifying a date from the past.

d. The path - together with the domain name, it specifies the path in which the cookie should be returned. The default is the path from which the file was sent.

e. The domain

The domain contains the address of the server from which the file is sent to the browser and to which it will be returned. The default is determined by the server from which the file is sent. There are systems consisting a number of servers and the file should be returned to all servers, and not only to the one from which it was sent. In this case the SubDomain is checked to see whether it contains the Domain that created the file; therefore this part should have two dots in the domain name for addresses ending with .net, .edu, .com, .org, .gov and for others - three dots.

f. The need for a secure connection for using the cookie

These guarantees that the cookie file is sent and received only if an SSL (HTTPS) protocol is used. The default is False.

An example of set cookie:
Set=Cookie: foo=bat: path=/: expires Mon, 09-Dec-2002 13:46:00 GMT

Types of cookies
There are two main types of cookies:

1. Session, Transient Cookies

Cookies loaded to the computer memory only while the user is surfing and are deleted once the user closes the window and stops using the web page. Such cookies are not saved to the hard drive and do not collect information. Therefore they usually contain the user profile for a specific site only - an ID, in order to avoid having to login. Such cookies are common on commercial sites as they can remember the products purchased.

2. Permanent, Persistent Cookies

Cookies loaded to the hard drive and not deleted when the session ends. They remain in the memory for a long period of time that can last several years. Therefore these cookies are permanent and can serve two purposes: first, like temporary cookies, they
identify the user. Second, they follow the user's preferences on certain sites and use that information in future. Therefore such cookies can give the site owner information on all of his users: how many visited the site, how much time on average they spent on each page etc.

The uses
Cookies have the main purpose of improving the surfing experience both for the users and for the sites that use them. For example, the user does not have to identify himself on every visit to the site - he is already identified. The site can also present contents suited to the user's preferences, whether his declared preferences or derived from analysis (personalization).

The Privacy Problems
The way cookies are designed and their technological uses cause problems: first, information on the user's activity is gathered, usually without his consent or knowledge, which violates his autonomy and his privacy. Browsers do allow for blocking cookies, which gives the user control. However in the current reality blocking cookies substantially reduces the number of accessible sites. It is also true only if we assume that the users are aware of the cookies, understand their significance and know how to delete them and succeed in doing so. A more serious problem arises when small and seemingly negligible pieces of information are gathered from several websites and cross processed in order to build a profile of the user's activities. Such a profile can teach us a lot about the user and may include personal information. Building such a profile requires processing and analysis, yet we should be aware that it is possible. In addition, the use of cookies compromises anonymity on the web: the possibility to identify the user with a cookie removes the partial anonymity of the user.

b. Web Bugs
A web bug is a graphic element appearing on a web page or an e-mail message, built in a way that makes it possible to monitor the activities of the person reading that page or message and the collect statistical data, mostly by third parties, especially advertisers. Web bugs are very small (1x1 pixels) and invisible. They are often planted on web pages by parties that collect information for the purpose of potential
market segmentation. They do this by sending a request to a third party. The web bug sends the request to the third party and this is considered a "hit" for the collector. This request provides him important details on the user's activities.259

The name is borrowed from spying terminology, from the name of a tiny tapping device. Other terms with the same meaning as web bug include Clear GIF (a transparent GIF image), beacon GIF and invisible GIF.260 The use of a web bug requires three computers: The user's computer visits a web page where the web bug is planted and automatically tries to fetch the graphic element. During this attempt, the user's computer contacts the computer of the site on which the page is situated and that computer sends it to receive the information from another site - the bug's site. This whole process occurs without the knowledge of the user, who does not see any of what is happening, as all the graphical elements are tiny.

This is what the web bug looks like when planted on a web page:

```
<img src="http://www.commission-junction.com/banners/tracker.exe?AID=14658&PID=259294&banner=0.gif" height=1 width=1 border=0>
```

And in an e-mail message:

```
<img width='1' height='1' src="http://www.m0.net/m/logopen02.asp?vid=3&catid=370153037&email=SMITHS%40tiac.net"alt=" ">
```

The information that the web bug contains include the username and at least six more items:

a. The user's IP address
b. The URL of the computer on which the web bug is installed
c. The URL of the web bug, including the information linking between the web page and its author
d. Information on the browser that operated the web bug: type, screen resolution etc.
e. The value of the last cookie on the domain.

Web bugs have several possible uses:

On websites:

259 Garfinkel, supra note 254, at 224.

1. Segmentation and profiling of a person's surfing habits. The personal profile is collected by cookies or other means of surveillance and after processing the information, web bugs that suit the profile are planted.

2. Service for the site owners - monitoring the number of visits.

3. Collecting statistical data on the manner and extent of usage of the browser.

4. Monitoring the efficiency of banners: did the advertising lead to growth in the number of visits on the sites directed to, has the demand for the advertised products grown, etc.

5. Monitoring a user in order to reveal his identity. This cannot be done, for example, if the party is not the operator of the forum. If a person is slandered on the Internet and the only information he has is the e-mail address of the party responsible, an e-mail containing a web bug can help him obtain more details.

**On e-mail:**

1. Finding a user who wishes to remain anonymous, as one who opened and read the message sent to him.

2. Statistical analysis of the number of times a message is read and re-opened (or deleted or viewed only once).

3. Comparing information on an anonymous to information on a non-anonymous user. Data cross processing makes it possible to reveal the identity of a user who uses two different nick names on a forum, or two different e-mail addresses. The information received, includes the IP address, the time when e-mail messages are read and the cookies installed.

4. Finding whether a user with a certain e-mail address exists and reads the email. Spammers remove from their databases those who do not read their spam, but usually, if you read their message once, you will continue to receive spam.

5. Synchronizing the user's cookies with a real address that he uses. For example, websites that require e-mail registration and those that do not can verify and collect e-mail addresses of users who visited their site and a cookie was saved on their computer and with an e-mail they read.

**The Privacy Problems**

The structure and technological uses of web bugs cause problems: we can compare a we bug to sending a registered letter with confirmation of receipt through the postal
service - when a person, institution or court send such a letter, the recipient must sign a document indicating that he received the letter, which is then sent to the sender, and the sender thus knows when the letter was received and the name of the mailman. The web bug operates in a similar way. However, with ordinary mail, the recipient is aware of the process and confirmation and gives his consent by his conduct, while he is not aware of the web bug and cannot consent to it.

**Comparative Law**

**United States**

The issue of using means of surveillance on the Internet was discussed in the *Double Click* case. The defendant was a company dealing with targeted advertising on the Internet. The focus groups were compiled by gathering information received from cookies and web bugs, processing it and analyzing it in order to prepare personal profiles of users and match adverts to those profiles. The plaintiffs argued against the manner in which the information was collected, relying on the causes of unauthorized access to computers, forbidden secret monitoring, abuse of a computer, unjust enrichment and trespass. All of these were rejected. In the U.S. there is no general protection of privacy and the cause mentioned could not form a substitute. It was held that collecting information in the manners described does not violate privacy and that these new aspects should be regulated by the legislator.

In a series of cases on the subject, the plaintiffs failed to prove the illegality. In the U.S. private law does not protect privacy (unlike EU law, for example), but there is a limited series of cases in which privacy is protected. In each of these the protection includes a great number of exceptions and reservations and thus creates a legal framework which is hard to enforce, complex and not particularly effective. The specific protections of privacy include, for example, protection of economic information with regard to credit cards and protection of information on rented

---


Europe

Unlike the U.S., the European Union recognized the potential problems raised by technological progress back in the 1990s and acted towards regulation in this field. In 1995 the EU adopted a directive on protection of personal information, under which within three years all EU countries had to adapt their legislation to its provisions. On 23 February 1999 the EU commission published its recommendations on protection of privacy on the Internet, applying the laws on privacy protection to the online world, the guideline being that communications using new information technology should respect human rights and basic liberties in general and the right to privacy established in section 8 of the European Convention on Human Rights in particular. In addition, the provisions of the Strasbourg Treaty of 1981, dealing with protection of individuals against automated processing of personal information, apply to collecting, processing and transferring personal information through the Internet. The recommendations stress the risk to privacy and recommend to both users and ISPs to use technological measures as possible solutions. A special recommendation directed at ISPs is to secure the information by physical and logical protection of the computer networks. That also encourages the ISPs to inform the users of the risks before they register for service and require them to give users information on the possibilities for access and anonymity online.

The Directive sets several conditions to guarantee protection of privacy on the digital age: personal information must be processed fairly and lawfully, collected for a specified, explicit and legitimate purpose, its processing must be adequate, relevant and not excessive in relation to the purpose, accurate and, when necessary,

268 Art. 6.1(a).
269 Art. 6.1(b).
270 Art. 6.1(c).
kept up to date,\textsuperscript{271} and it must be held no longer than is necessary for the purposes for which the data was collected.\textsuperscript{272}

The most significant requirement is that the information can only be gathered if the user has unambiguously given his consent.\textsuperscript{273} Unlike U.S. law, the exceptions under European law are few: public interest,\textsuperscript{274} a vital interest of the data subject,\textsuperscript{275} or no fundamental privacy interests of the data subject being at stake. In addition, the Directive contains a broad discussion of data classification and therefore also of sensitive personal data,\textsuperscript{276} in relation to which there are no exceptions:

1. The data subject has given his explicit consent to the processing of those data, and had the legal right to consent;
2. The data processing is necessary for a lawful purpose.
3. The processing is necessary to protect the vital interests of the data subject or of another person where the data subject is physically or legally incapable of giving his consent;
4. The processing is not carried out for non-profit purpose and the data are not disclosed to a third party without the consent of the data subjects.
5. The processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims.
6. With regard to medical information, further limitations apply, regulated by medical laws.

Moreover, the directive supports the view that the data subject owns the data, and grants access and a legal right to any person to view the data, examine the reasons for its collection etc.\textsuperscript{277}

\textsuperscript{271} Art. 6.1(d).
\textsuperscript{272} Art. 6.1(e).
\textsuperscript{273} Art. 7(a).
\textsuperscript{274} Art. 7.
\textsuperscript{275} Art. 8.
\textsuperscript{276} Art. 10-12.
\textsuperscript{277} DN 9/83 Military Appeal Tribunal v Vaknin, 42(3) P.D. 837.
Israel
Under section 2(1) of the PPA, privacy is violated by "spying or monitoring a person in a manner that might harass him, or by other types of harassments." Apparently, this section can be applied to monitoring the activities of online users, yet it is doubtful whether the element of harassment exists. However, we must ask ourselves whether sending cookies or web-bugs can fall under the legal definition above. On the one hand, the cookie and the web-bug do not harass the user, but have the potential of helping him surf more conveniently (e.g. list of advantages). On the other hand, the cookie and the web-bug, as they are used these days, are declared means of monitoring.

Section 2(5) of the PPA forbids copying the contents of a letter or other things in writing not intended for publication, or using their contents, without permission of the author or the recipient. On the common fears in the digital environment is of information collected by cookies or web bugs. The question is: are these other things in writing not intended for publication? Obviously answering this question in the affirmative is not a trivial matter.

Section 2(9) of the PPA provides that use of information on one's private matters or transferring it to another for a purpose other than that for which it was originally given, constitutes a violation of privacy. The case law on this matter held that even using a person's name, address, telephone number and such other details, should be considered information on his private matters. In the digital world, with the architecture of the web as it exists today, some details collected about a person on one site may find their way to another site. It appears that in such cases, where a person gives his details to a store in order to purchase a product, and the information is used in order to display advertising suitable to him on a different site, section 2(9) applies.

The problem presented by cookies and web bugs is that the more hidden their activity, the harder it is to consider the user as having "given" the information. Does a user give his implied consent to the technical aspects of the Internet, including

278 Database Registrar v Ventura, 48(3) P.D. 805.
279 Haim Ravia, Privacy on the Internet (Part 4) 
cookies and web-bugs? If a user does not restrict their activity, should this be seen as implied consent to collecting the information they contain?

It should be noted that the uses made of information collected by cookies and web bugs are subject to the provisions of the PPA. For example, giving the names of people who visited a sex site to suppliers in this field is prohibited, because such information can be seen as intimate. ISPs are under duty to hold a license for operating databases containing information collected by these means.

c. Sniffers

A sniffer is a piece of software that captures all information to and from a computer connected to the network. Sniffers have several versions, some commercial and some created by hackers. Some sniffers are in the form of hardware with matching software and some are part of the computer's electrical cycles or ROM memory and cannot be changed. While performing routine activities online, such as surfing and communicating with other users (for instance through e-mail), computers have a constant communication with other computers. Most computers these days are connected to each other through a Local Area Network (LAN), sharing one connection to the network with other computers in the same building. The local area network makes it easy for sniffers to operate, as the information directed for one computer is transmitted to all computers on the same local network, unless switches are used on that network. This means that every computer on the network "sees" the information to and from the other computers, and it normally ignores such information, unless it is instructed otherwise. The sniffer, placed on a switch or on a router, "tells" the computer's NIC (Network Interface Card) to stop ignoring the information traffic directed to all other computers, by changing the NIC's mode to

---

280 See chapter 1.c (The Element of Consent) above.
281 Section 11(2) of the PPA.
282 Chapter B of the PPA.
285 A switch is an external device used on local networks in order to direct information packets through the network. Sniffers can also be used against individual users, but information belonging to organizations and corporations is usually more important.
286 A router is a computer that directs information packets to the available segments within the local or general network. See: A Beginner's Guide to the Internet, http://www.securityfocus.com/infocus/1180.
promiscuous mode. This can only be done by the network administrator, to whom the network belongs or who is appointed by its owner to operate it. Thus the sniffer can "see" all the information in the part of the network where it is placed and systematically reads all such information. The sniffer "pills off" the covers of the packets of information transferred and decodes their contents, as well as the IP address of the computers participating in the transmission. Some sniffers identify only information sent using TCP/IP but man can operate with other protocols too, such as on Ethernet frame.

The Dangers to Privacy of End Users Presented by Sniffers

On a standard local area network thousand of information packets are transferred between computers, susceptible to sniffers. Plain text is vulnerable to attack by sniffers, including passwords, web pages, various messages etc. The sniffer can be designed to capture specific information, such as telnet texts or e-mail. Databases are also desired by sniffers, used mostly for commercial uses, such as spam. Once the information is received by the sniffer, its operators can rapidly collect the information they need, such as logins, passwords and texts, without the end user's knowledge. Among the hostile parties that may benefit from the use of sniffers are hackers, nosy colleagues and business rivals searching for trade secrets.

Undoubtedly the means providing the best protection against exposure of information is encryption by various methods, which can guarantee to a high probability that the recipient is the only one who can read the information sent to him.

Can sniffers benefit us? They definitely can. Sniffers can, and were originally intended to, be used by system administrators, network security experts and programmers, as they provide reliable information on the flow of information on the network, unlike other means that view the network from the outside. For example, a system administrator can ensure that the network is functioning properly. Also, in the creation of web applications the use of sniffers is vital to prevent virus infections during development. Amateur users may also find interest in sniffers in order to understand how the network operates.

Following the events of September 11, 2001, the FBI developed a sophisticated sniffer called Carnivore,\textsuperscript{287} in order to scan e-mail messages and other electronic

\textsuperscript{287} Supra note 63.
correspondence. In theory, it is capable of "sniffing" millions of e-mails per second, and about 6GB of data in an hour, and it can also locate within that enormous amount of data the information it evaluate as necessary for the investigation, download it, explore it and then return it to its route. Computer security experts assume that the FBI places the sniffers on the servers of the ISPs, so as to have access to the maximal amount of information. The only US ISP cooperating with the FBI is Earthlink, and as a result there have been some problems with its customer service.288

There are several technological means for protecting against sniffers. First, system administrators must secure the main computing systems and the network servers. Second, various programs can be used, such as "Antisniff", that scans the network in order to determine whether the NIC is in is promiscuous mode. Such check should be made on a regular basis as they function as "alarm" alerting from unwanted sniffers. Also, when the LAN switch is off the information packets are sent only to and from the recipient and not to or from all other computers on the network.289

Spyware

One of the first definitions of spyware was suggested by Steven Gibson, one of the leaders of the fight for privacy on the web:290 spyware is any program using the Internet background connection without the user's knowledge or explicit consent.291 Spyware is a generic name referring to software "planted" on the end-user's computer in order to collect information on his surfing habits, for advertising supported software or other interested parties.292

Originally adware programs (such as Go!Zilla) were called spyware. These are known in the field of Internet advertising as "infecting" computers with adverts. However, the novelty of the first spyware programs was the installation of an adbot component, by advertising company Radiate (which was called at that time Auriate),

289 Using a program such as Dsniff it is possible to monitor information using a technique called Arp-spoofing, with similar results to sniffers. Another option is to use modern sniffers, such as the sniffer described on this page: http://ettercap.sourceforge.net/.
291 The computer background is the environment in which secondary activities take place alongside the main application. Hackers' slang refers to it as "Backchannel".
aimed at displaying adverts on the PC. This component would run in the background even when the program (Go!Zilla) was shut down, using the Internet Explorer browser to download and update adverts, and to report on the adverts viewed by the user, the ones he clicked and which software he used. When the user ran the program that installed the adbot component, the adverts would appear on the screen so that the advertisers knew how much to pay the adware operators and how much they should be charged, in accordance with the numbers of views and click-troughs.

When users and various bodies (mostly in the U.S.) discovered this, it raised protest and they set up websites on the subject, where antidotes can be found; some programs were developed in order to block adware and spyware (some distributed for free) and the term "spyware" received bad publicity. Later on different names were attached to those programs, leaving no room for doubt about their nature. Today "spyware" is a general name for any programs that spy, including the main applications details below.

How Spyware Operates
The spyware programs start running when the operating system loads and once the computer is turned off, they create unauthorized proxy servers on the end-user's computer, designed to disguise the activity being carried out through the network connection. Then they download adverts onto the computer (such as DoubleClick, Web3000, Radiate, SaveNow, GAIN), and some access the history files saved on the computer to find the sites the user visited, the number of visits etc. (such as Toptext, Cydoor, OnFlow, Medialoads, Delfin, WebHancer, New.net). The aim is to create a profile of the end-user for commercial purposes. These programs include a mechanism through which they are constantly in touch with the "headquarters" (the ad serving networks) and deliver the information by sending a unique encoded transmission to each computer.

As already noted, the aim of these programs is to monitor and follow the uses of the end user, online and offline. However, beyond the obvious violation of privacy, and sometimes compromise of his property rights, there are many side effects, some

293 Among them such names as: parasites, unsolicited bulk downloads, unsolicited commercial software and potentially unwanted programs.
294 http://www.simplythebest.net/info/spyware.html.
295 Ibid.
of which are not even planned to accompany the spyware. Among these are "security holes", making it possible to install more programs on the user's computer; slowing down the computer and reducing it performance; sending and receiving cookies and Trojan horses to and from the spyware installed on other computers (even if they are geographically remote from the user's computer, and regardless of his settings with regard to cookies); reset log password of the computer; stopping devices not yet installed on the computer and scanning, writing and formatting files on the hard disc.\textsuperscript{296}

Moreover, any attempt to remove the spyware is reported to the headquarters and even if the user managed to remove it in some way, it leaves certain components behind, which enable it to continue operating and sometimes re-installed.\textsuperscript{297} In more serious cases, but not as rarely as they may seem, the attempt to remove a program with many components may lead to damage to the operating system, instability, inability to use the mouse or keyboard (usually temporary) and sometimes it may paralyze the computer.

Apart from the spyware mentioned above, there are three other main types of programs, sometimes classified as spyware:\textsuperscript{298}

- **Pop ups**: open a window in the web page or in a new page by advertisers and porn sites.
- **Dialers**: connect the user's modem to the modems of porn sites and gambling sites (usually outside Israel) and charge the user for the long distance call.
- **Homepage hijackers**: change the browser homepage to a different page chosen by the advertiser and sometimes add new sites to the list of favorites.

The activities described are sometimes not in full conformity with the declared privacy policy of the advertisers involved.\textsuperscript{299}

\textsuperscript{296}http://www.dokdesk.com/parasite/.

\textsuperscript{297}http://www.simplythebest.net/info/spyware.html.

\textsuperscript{298}These are mentioned in order to present the full picture on spyware, although the use of these programs does not amount to spying, but forms a nuisance.

\textsuperscript{299}For example, Gator's policy on this page: http://www.gainpublishing.com/help/websiteandterms/. The company claims that it gather data (IP address, browser, software installed) on users who installed its software and shares it only with its employees and authorized persons, yet it does not explain who the authorized persons are.
It is important to note that spyware is not a computer virus, as its purpose is not causing damage, but gathering information and because it lacks the inherent characteristics of viruses - anonymous creators.

How Does Spyware Reach Us?
There are several main sources of spyware: Firstly, through freeware, including P2P programs such as Kazaa, an earlier version of iMesh and Grokster, whose distributors also distribute registered programs for sale. The free versions are preferred by the average users, but here lies the trap, since the programmer needs to return the investment. The freeware is not paid for with money, but the end-user pays for it by waiving his privacy to some extent.

The main problem is that the installation of adware is initiated by the end-user with his full knowledge, while he is normally unaware of spyware being installed on his computer. Even if it is mentioned in the installation agreement, he would normally not notice the small print, since the agreement is too long and normally cannot be fully understood by the lay user. In practice, even though the average end-user might have agreed to the deal, he was not given a real opportunity to refuse it. Naturally, entering into an agreement in such circumstances raises a question about the validity of the installation agreement (see the chapter on The Element of Consent).

Secondly, when a web page has a link to an ActiveX program, a window opens on the page asking the user is asked to consent to the installation. If he hastily clicks "yes" (or if the security options are set to "low", so he is not asked at all), the program can run on his computer. Sometimes sites or pop up windows tell the user that installing a program is required in order to view a site, or that the digital approval in the code mentioned on the page indicates that it is safe for use. If he refuses to install it, he is likely to have a series of pop up windows on his screen, when closing one window makes several other windows open, and so on.

Thirdly, installation using browser security failures while getting the code needed got running the programs. Although the Microsoft Corporation provides its clients with regular updates that can be downloaded from its website, there are still

---

300 A computer virus - software that distributes itself among as many computers as possible, reaching them in several ways: files exchanged between users, e-mail, cracked software etc.

301 Although today most adware programs are in fact spyware.
"security holes" that have not been fixed and are frequently exploited by different parties.  

**Are there positive uses for spyware?**

The answer to this question, surprisingly, is positive. The Microsoft Corporation uses a component of spyware called Browser Helper Object (BHO), which the Internet Explorer browser loads when it starts running. This program can perform any action in Windows and in the available modules, including reporting on different events that occur, creating windows in order to display further information on the page being viewed, monitoring actions and messages and so on. Microsoft calls it "a spy we send to infiltrate the browser's land." However, that same component is often exploited for some of the activities described above (such as homepage hijacking, scanning the history files etc.)

**Protection against spyware:** there are several technical means the end-user can use in order to protect himself or herself against spyware. In addition, he or she had better verify that it is indeed spyware. There are many sites that provide up to date spyware lists. Fire Wall programs are highly recommended. They provide a "wall" between the end-user's personal system and the network. In some of these the user can define the level of protection he is interested in. There are also programs that find and remove spyware, such as SpyBot and AdAware. Ordinary anti-virus programs are insufficient for this purpose, as they only remove the programs they were "taught" to identify, and in the case of spyware these are only few of them.

However, the main disadvantage of the programs mentioned above, including fire wall, apart from the fact that they do not identify all spyware, is their cost that can reach a few dozens of US Dollars. This is a substantial amount of money, given the

---

302 One solution is to set the browser security level to "high", but this would make surfing difficult as many sites will not load.
303 A module is part of a computer program that can be run separately. Jay Munro, "Security Watch Letter: Lovgate is a Quiet Yet Dangerous Lover", PC Magazine, 06.07.2004.
304 [http://www.pcmag.com/article2/0,1759,1620249,00.asp](http://www.pcmag.com/article2/0,1759,1620249,00.asp) (last visit 20 March 2005).
305 For example, it is recommended to change some default preferences: remove unnecessary protocols such as (NetBIOS/NetBEUI), change the Print & Sharing Files default preferences, change browser preferences and disable the "Enable hit page counting" and "Enable cookies" options.
306 See for example, [http://www.cexx.com](http://www.cexx.com), and Gibson's website mentioned above.
307 Business and public systems had better purchase VPN system, providing high levels of security. One of the leading companies in this field is Check Point: [http://www.chek-point.com](http://www.chek-point.com).
fact that the competition between the developers of surveillance and protection programs is a never ending one, and this is partly sue to the fact that sometimes they are the same companies. Yet there are less expensive practical alternatives the end-user must read every document in which he is required to confirm the installation of any software. The browser security preferences should be set to "medium" at least, in order to receive an alert in case of an attempted break in. Obviously, the main problem is the lack of awareness of users to the existence of these programs, their activities and its meaning. We cannot say the user "consents" to such activities, and therefore the issue of consent is so important in the legal discussion.

e. Trojan Horses

Trojan Horses are programs installed on the target computer and give the creators a "back door" through which they can enter the computer without limitations. Unlike spyware, the victim is not supposed to know the identity of the parties involved. We shall distinguish between several categories of Trojan Horses, according to their activities and functions. One Trojan horse can belong to more than one category.

Remote Access Trojans

Most Trojan horses belong to this category. They grant complete control over the victim's computer, including access to files, finding credit card details, passwords and e-mail addresses, as well as passwords for Internet services, confidential documents and drawings, images etc. These programs consist of two parts: the client program, installed in the destination computer and the server program on the attacker's computer. The attacker runs a scanning program, such as Port Scanner, to search for open ports in the network, or known loopholes in the operating system, unprotected accounts and back doors to the system. In the next stage the Trojan horse invades the computer and sets itself as its administrator. When the user uses the client program and enters the IP address, the server receives instructions from the attacker and performs them. Some Trojan horses make it possible to change the port or set a

309 Through a virtual port information passes in and out of a computer according to protocols. See also: http://www.halemo.com/edoor/0045/mossad.htm.
password so that only the attacker can use the computer. In some cases he may also leave himself away to access any computer on which the server program runs, without using a password (a Trojan within a Trojan).

After installing the client program and obtaining the user's IP address the attacker can gain control of the computer system files (the hard disc and its entire contents), and he may use various programs in order to hide his tracks like deleting log files, system files and security preferences. Trojan horses in this group include: Trojan Back Orifice, Sub7, Netbus.\(^{311}\)

**Data Sending Trojans**

These Trojan horses log every key the user types using his keyboard and save it in a hidden file.\(^{312}\) These are called Key Logger Systems (KLS).\(^{313}\) The information gathered usually includes passwords (for e-mail, ICQ and IRC),\(^{314}\) access codes, e-mail messages, chat transcripts, credit card numbers, sensitive business correspondence etc.\(^{315}\) Certain Trojan horses are even able to follow the end-user through the web cam connected to his computer.\(^{316}\) The information gathered in the file awaits its future dispatch to the party gathering the information or in some cases delivered to them immediately with the raw material it contains.\(^{317}\) The file is sent using the end-user's e-mail or a link to the attacker's website. He the reviews the information, hoping to find passwords or other useful information in order to perform credit card transactions, steal identities or perform a social engineering attack.\(^{318}\)

\(^{311}\) [http://cybercrime.planetindia.net/trojans.htm](http://cybercrime.planetindia.net/trojans.htm).

\(^{312}\) Another less common type of keylogger is a device connecting the keyboard to the computer port, see for example [http://www.keyghost.com](http://www.keyghost.com).


\(^{314}\) ICQ is an instant messages program, used for conducting "conversations" on the users' computer screens by sending and receiving messages in real time. IRC is a chat service creating virtual meeting places in which people from all over the world can meet, share files and exchange correspondence.

\(^{315}\) Roy Shlomi, “A Guide for Beginner Paranoids” (Hebrew) [http://www.ynet.co.il/articles/1,7340,L-2825399,00.html](http://www.ynet.co.il/articles/1,7340,L-2825399,00.html).

\(^{316}\) This option appeals in particular to employers wishing to spy on their employees. See: [http://www.jobinfo.co.il/Content/Career/Politics/avoda4.asp](http://www.jobinfo.co.il/Content/Career/Politics/avoda4.asp) (Hebrew).

\(^{317}\) [http://www.pestpartol.com](http://www.pestpartol.com).

\(^{318}\) “Social engineering attack” is a term used by hackers describing breaking into a computer based human error in securing the system.
Proxy Trojans
These Trojan horses turn the computer under attack into a proxy server, and thus make it available for use of the entire user community or the attacker himself. It is used for anonymous conversations on telnet, ICQ etc; credit card transactions and other illegal activities. The actions of such Trojan horses grants the attacker anonymity and complete freedom to act as he wishes using the end-user's computer, including attacking other computers. Thus, in case his actions are discovered, the footprints lead back to the innocent end-user.

FTP Trojans
These Trojan horses open port 21 used for exchanging FTP files and this enable the attacker to connect to the computer through FTP.\textsuperscript{319}

Trojans that paralyze security programs
These Trojans stop or destroy security programs such as anti virus, firewalls etc. in order to allow the attacker to operate without interruption. Often there Trojans accompany viruses, for example the GONER worm that attacked many computers around the world in December 2001 included a Trojan horse of this kind that deleted anti-virus files. The use of is Trojans is normally directed against individual ed-users, rather than collective systems.\textsuperscript{320}

There are two main ways in which Trojan horses can break into a computer or a computer system.\textsuperscript{321} First, by e-mail attachments sent to the end-user. When the end user opens the file, the Trojan horse enters into his computer, and on a local network it can also invade all other computers on that network. The attacker would normally try to tempt the end user into opening the e-mail message, for example by making him believe it was sent from a destination that may profit him. In some cases he may use the name and e-mail address of a person whom the end user knows. If the end user does not have a security program for his e-mail software to discover security loopholes, the e-mail attachment can load automatically without intervention by the

\textsuperscript{319} FTP (File Transfer Protocol) is a communications protocol used for file transfer.

\textsuperscript{320} \textit{Ibid.} In February 2003, the Israeli youth who programmed and distributed the GONER virus were convicted under section 6 of the Computer Law. See: \url{http://www.bsh.co.il/ShowArticle2.asp?ArticleId=194&CategoryId=23} (Hebrew).

\textsuperscript{321} Assuming the system is protected by firewall and the ICQ and IRC programs are not connected.
end user. Second, by downloading files from web pages. This is similar to spyware infection, is the user visits a certain website, and downloads a program he is interested in, in which the Trojan is installed. For example, ZeroPopUp Trojan was presented as a program blocking pop up windows. The attacker spammed any end users and described the virtues of that program, asking them to download it through the link provided. Many recipients were tempted to install the program.\(^{322}\)

Protection against Trojan Horses

As with spyware, anti-virus programs cannot normally detect most Trojan horses.\(^{323}\) The problem is even worse with Trojan horses, as their codes are readily available online. As a result, any skilled attacker can create a "mutation" of a certain Trojan, change its personal code, so that the anti-virus program will not be able to detect it. Therefore a multi-phase strategy should be used in order to efficiently protect the computer against Trojan horses.\(^{324}\)

Positive uses of Trojan Horses

The only beneficial sue of Trojan horses for remote control is for the end user to control his own computer. Yet since there are programs for this purpose on the market,\(^{325}\) installed by the user with full knowledge and intent, and since this type of use is not practically performed by Trojans, this advantage should not be attributed to the Trojans only.

Data sending Trojans may have several positive uses. First, they can be used by the police and other law enforcement authorities to investigate computer fraud or finding passwords for encoded information required for investigation. Secondly, system administrators wish to monitor unauthorized use of the network or parts of it by hostile parties. In addition, theoretically, the keyboard loggers can collect statistical data about the use of the computer. The employer can use this to deter

\(^{322}\) *Supra* note 311.

\(^{323}\) Therefore in order to trace most Trojans the user needs several anti virus programs. For most users this is a substantial expense.

\(^{324}\) *Supra* note 311.

employees from undesirable use of the company's resources; finally, the end user has another option for saving backups of the information on his computer and to know whether his computer is used without his permission, and if he is a parent - to endure that they use the Internet in a safe and appropriate manner. Of course, against all of these is the user's right to privacy.

F. Means of Surveillance on the Cellular Network

The Cellular Space

Mobile communications quickly became part of our lives and today over 40% of the computer and telephone communications is performed using mobile technology. Every two seconds a new cellular device (hereinafter: the device) is added to community of cellular users the in the US (hereinafter: the user). At the end of the day, tens of thousands of new Users join over existing 100,000,000 Users in the U.S. Experts estimate that by the end of 2005 there will be over 1.26 billion Users worldwide. In Israel the rate of penetration of cellular devices to the 12-30 year of sector is 84%. This sector constitutes 31% of the population.

Cellular network operates can reach by rather simple means information on the Users' conversations, including the phone numbers, the time when it took place and how long it lasted and the locations of the participants. The speed with which technology for locating Users is developing rapidly in the past few years. With the convergence of Internet and cellular phones and especially "third generation" devices, equipments are being developed that will lead to increases use of mobile internet. This technology makes it possible to locate the user more easily. How does the technology work? First we shall describe the operation of the cellular network

| The cellular system divides each area where service is to be provided and antennas are positioned in it. The mobile communications are conducted only between the device and the cellular antenna from which it is transmitted to the switches. The switches |

326 Supra note 311.
327 http://www.bynet.co.il/magazine/asp.
328 Data presented by CTIA as of November 2000: http://www.ctia.org/.
329 Shlomi Doner, "Survey: 60% of 12-16 year olds have a cellular phone" http://www.ynet.co.il/articles/1,7340,1-2808138,00.html.
direct the call to the switch relevant to the call destination within the network or in another network. The operator's switches produce unique information called CDR. It contains the information typical of any linear telephone network and in addition - the user's movement, according to the antennas.

Therefore the operator can know what you say and where, by:

A network based on triangulation: in the first stage three radio signals are collected from the three cellular antennas closest to the device. In the second stage the relative location of the device between the three antennas is calculated, which enables to locate the user. The common technique is to calculate the distance between the device and the antennas using the speed of the wave transmitted by the device.

Global Positioning System (GPS): 24 special satellites broadcast their geographical location constantly. At the same time the cellular device has a GPS processor that sends transmissions to the satellite, with information on the user's location. The satellite sends them back the devices that inform of the user's location.

The uses of the Technology

The technology for locating the user is used both for security purposes and for commercial purposes. In Israel the technology had been used for security before it was used commercially. The dynamic development of this technology and the large extent of the cellular devices market penetration worldwide lead to many modern developments in this field and to unforeseen problems. Following are some of the uses of the technology:

1. **Monitoring.** The operator can be constantly in contact with the device, so the user can be traced at all times, even when the device is turned off. This becomes more complicated in non urban areas where there are fewer antennas.

2. **Profiling.** Gathering information on the user and creating a user profile for commercial purposes. The marketing company can address the user with offers for

---

330 Call Digital Record.

products he is interested in, thus the use enjoys direct marketing of the products he wants and the seller increases his sales. Apparently, both parties benefit from this, but we should remember that the gathering of information is not always conducted for positive purposes.

3. Monitoring by local operators is possible by using computing equipment at the call operators of the operators or by satellites.

4. Mobile advertising. Since 2000 it has been possible to surf the Internet through cellular devices and the methods for gathering information online are coupled with the methods for gathering geographical information. By locating the user near a business, it is possible to send advertisements such as SMS messages, message sent through XHTML sites and MMS with photos, music or video clips.

**Advantages:** the commercial uses of the technology are evident in the speed of information transfer, its availability and its adaptation to the user's location, allowing him to save time, in addition the technology answers security needs by helping tackle terrorist organizations.

1. The use for security purposes is the main advantage, as it enables the prevention of terrorist attacks. For example, when the intelligence knows of a terrorist planning a terrorist attack, it is possible to locate him, it also enables to locate a person in emergency situations by the police, fire fighters, etc, as the device can be located even when it is turned off.

2. Creating a database to assist with enforcement, in order to locate criminals by monitoring their calls and locating them. This can also be used in order to locate stalkers (Prevention of Stalking Law). However, the operator should not be turned into the long arm of the enforcement authorities of private parties.

3. An up to date service for the use, for example - receiving localized weather reports, traffic jam reports and local news.
4. Personalization of marketing messages,\(^{332}\) by matching the user's areas of interest to his location. For example, a user interested in sports can keep up to date on the sales offers at the sports shops near him. Obviously overusing this option and impermissible marketing can derogate from this advantage.

5. Credit card security - financial bodies can easily locate users from countries where forgery of credit cards are common or send a warning when a refrigerator is purchased on the Internet with an American credit card when the user is in India. Thus technology promotes information security and protection against fraud.\(^ {333}\)

**Problems raised by use of the technology:** the cellular technology has many advantages, as described above, by some of these are problematic. The technology enables progress, using time efficiently and greater security, yet it raises some technological and legal problems.

1. Violation of the user's privacy - the technology described violated the user's privacy in two ways: first, gathering information on his location at any given time and cross processing it with further data, such as his name and his age, create a user profile, which may be incorrect, as he may be at a certain location by chance only. Secondly - the use does not consent to the use of the technology in such a way, as he often does not know that such information is gathered. After the information is gathered by the operator, it can also be given to third parties, which is problematic in itself, and the problem is even more severe, as the use has no ability to supervise the use of the information about him. When the operator stores the data for an unlimited period of time, it creates an enormous database. The information may be given to third parties for commercial purposes or even to the state (under a court order).

2. Lack of interest on behalf of the players in the field (the operator, the user, the public, the stat). The state obliges the operator to sign a secret security appendix as part of its license and has a direct interest in silencing his matter.\(^ {334}\)

---


\(^{333}\) Such a serve is provided by a company called Quova [http://www.quova.com](http://www.quova.com).

\(^{334}\) See the lecture by Sharon Keren, Cellcom's legal department, Shfayim 2001. Cellcom has a license to provide the security services with special services.
surveillance options of the new technology will harm public security. On the other hand, private commercial bodies make use of this technology freely and with no supervision. The operator who is licensed by the state signs a secret declaration cannot raise this issue, and the uses of the technology have a significant economic value for him, as he wishes to reduce regulation and allow for the "flow on information" as well as his cash flow. The use who wishes to progress with technology and purchase the device becomes part of the consumer statistics. The operator does not ask for his consent and the ability to locate him remains an unchangeable default.

3. Technology development makes it easier to violate the right to privacy/ the globalization of cellular networks caused a shift from a small local network to a worldwide network. Similarly, the development of GSM technology, which operates almost everywhere in the world. It enables the use to call and transfer data anywhere on the network.335

4. Lack of consumer awareness - the information provided to the user about the advantages of localized services is insufficient, and even more so with regard to the disadvantages. This leads to a lack of awareness regarding the issue of privacy, as most people are unaware of the implication of surveillance technology.336 For example, a car hire company fined a driver for speeding, as was agreed under the hire agreement. The information about his speeding was received through the GPS device installed in the hired car, and the speed was calculated on the basis of its locations at different points in time. Apparently, this constitutes an invasion of privacy, as the driver was not told that he was under surveillance.337

5. Unjust Enrichment - a user profile based on cross-processed information is a valuable economic asset. When it is sold to third parties without the consent of the

335 Today sending a text message from one cellular network to another requires an agreement between the two operators, while using GSM the user can dial by entering the state code and local network code


337 James Turner v. Acme Rent-a-Car
data subject, without his or her knowledge and in violation of the right to privacy - this may be seen as unjust enrichment.

6. The operator becomes "the long arm of the law". In the absence of explicit legislation imposing a duty on the operator to assist in an investigation by violating users' privacy, it appears that the state cannot oblige an operator to do so. Moreover, the activities require resources and money and we cannot see the legal basis for imposing such a duty.338

7. Spam - excessive marketing message sent to the use.339

The Legal Situation - Comparative Law

The United States

The legal system in the US in the field of privacy protection with regard to telephone and data communications networks has greatly developed in the past few years. This is due to the development of awareness to the right to privacy. Different consumer protection bodies are more aware of the technologies that enable collection of information and act to protect consumer rights. In the cellular field, security considerations were the main cause for explicit legislation and regulation, on which we shall elaborate below. In reviewing the legal developments in the U.S., we chose to focus on the question of consent, as we consider it to be a key issue in the regulation of this field.

In 1996 the FCC began discussing the subject and issued regulations on localized services, in order to improve the emergency services, so that those who call them do not need to describe their location. This is a new type of legislation, based on security considerations, rather than commercial ones. This type received formal approval in October 2001 by the USA PATRIOT Act.340

In 1999 an act dealing specifically with this matter was enacted - The Wireless Communications and Public Safety Act of 1999 (WCPSA), referring to geographical location technology and thus extending the Telecommunication Act of 1996, in the

338 Netvision v IDF (unpublished) ISP Netvision was required to provide information on its clients, and it was a held that a private body should not be turned into the long arm of the law.
339 Supra note 184.
context of gathering and disclosing information under the CPNI, and it also included new sections regarding localized services. Under this act, other than emergency services, an approval must be granted by the user to use localized information. Despite the court ruling in the US WEST case, under the Act the user should give his "express prior authorization," namely, an "opt-in" consent. This way in which it is given was discussed in a conference held by the FTC in 2002, where it was agreed that the issue of consent should be presented in an unambiguous way by clear wording, easy to read and understand.

The European Union
The EU Data Protection Directive of 1995 is considered as most comprehensive legal measure and contains clear definitions about gathering data, processing it and disclosing it, about the parties permitted to engage in such activities and the need to obtain the consent of the data subject. The processing of data is lawful only where the data subject provides explicit consent, except where state laws provide that it is impossible to do so, or for other essential purposes, such as security and public health. It should be noted that the consent of the data subject is defined as a specific indication that he or she gave his or her free will consent to processing the data.

The European directive also provides that the data subject has the right to access the information and to know the type of information processed and to whom it is given. The data subject also has the right to object to the information being processes or to demand that it be updated before given to third parties. Under the directive, the states must enact or update state laws in accordance with the directive and the various states have done so.

The development of legislation in Europe in this context has been different and contrary, in terms of its source and trends, to the legislation in the U.S. While in the

---

343 Article 7.
344 Article 2.
345 Article 12.
346 Articles 14, 15.
U.S. the initiative was that of the FCC, a governmental agency, in order to promote the emergency service (E-911), before the market was ready for these changes, in Europe the cellular operators started examining, acquiring and operating localized services before the legislator, the intervention of the European Commission, which regulates these services and indicates the need to support the emergency services in this area.347

Generally, the Commission held that it is possible and even desirable to have all communications networks, linear or cellular provide the emergency services with the information in the user's location when he calls them. The Commission stresses the need for information security and protection of privacy in order to prevent unfair use or inappropriate use of such information.348

In the year 2002 a directive was enacted referring inter alia specifically to the localized services technology and to the cellular market.349 Under the directive direct marketing to cellular devices requires prior consent by the client, except where there have been prior consumer relations. Under the directive where such relations exist it is possible to send marketing messages but the client must be informed that he may refuse to accept the service (opt out). The directive also provides that whenever a commercial message is sent to the client, the opt-out offer should be sent with it.350 It clearly provides that the state is entitled to use the information on the user's locations for enforcement purposes and for information on traffic.351

The Existing Legal Situation in Israel
The Israeli legislator has not yet considered the protection of privacy on the cellular network, as a separate issue from the general PPA. A proposal submitted to the Knesset in 2003 was not accepted.352 These questions have not yet reached the courts.

347 The European Commission has been working for several years on comprehensive arrangements for change and liberalization in the communications market in order to open it to fair competition and enable it to face the rate of technological changes. See the 1999 Communications Review (COM 1999/539).
348 Directive, articles 2, 4, 5 European emergency call number.
350 Ibid.
351 Ibid, article10.
352 See the proposal PPA (Amendment - Transfer of Communication Data) 2003 under which use of data including the conversations and location of users should be considered as privacy violations.
We shall examine the current legislation and whether it is compatible with several issues: gathering information without the user's knowledge, processing the information and using it or giving it to other parties, the need for user's consent, the extent of the consent and its form.

The Computer Act of 1995 prohibits invasion into computer materials unlawfully. Section 4 defined such invasion through communication or by tuning on the computer. Does a cellular device constitute a "computer" under this Act? It appears that the answer is not clear cut, as some of the devices are not operated by software, but the technological development combining applications and software in a device indicates that it may fall under the definition of a computer. The "invasion" into a computer is performed, first and foremost, order to implement the cellular technology and the other purposes are only secondary. Gathering information is an integral part of the architecture of cellular technology. The difficulty is not only related to the gathering of information, but also to the use made of it, but the use is regulated by the PPA, section 2(9). It should also be noted that section 11 of the Computer Act, amending the Criminal Procedure Ordinance (Arrest and Search), provides that invading into a computer system constitutes a search, requiring a search warrant. It is of course doubtful whether gathering geographical information involves "invasion" into a computer.

The PPA provides that one's privacy must not be violated without his consent, and violation of privacy is defined in section 2(1) as, inter alia, spying or monitoring a person in a way that may harass him. The harassment is not is sufficiently clear, therefore we should examine which interests are protected. There is no doubt that locating the user is done without is consent, but the problem arises due to the fact that this is part of the ongoing data transfer by the operator as part of the service.

Chapter B of the Act provides a legal arrangement with regard to databases. It should be examined whether the data on the user's geographical location falls under any of the definitions of "information" under the Act (information is defined as data on a person's personality, personal status, intimate matter, health, economic situation,

353 See the definition a "computer" in section 1 of the Computer Law, 1995.
355 DN Vaknin, supra note 25.
professional qualifications, opinions and faith).\textsuperscript{356} We should consider whether the operator's database falls under the definition of "a collection of data held by a magnetic or optical device or intended for computerized cross processing, save for the exceptions under the law."

The Secret Monitoring Act of 1979 prohibits secret monitoring without the consent of the participants. The information is not gathered by one of the participants, therefore it falls under the definition of monitoring.\textsuperscript{357} We should also consider whether the use the operator makes of the location technology meets the threshold requirements for secret monitoring. It seems that since the contract between the user and the operator does not include any provisions on the matter, and thus the user is not asked to give his consent, the monitoring is done without his consent. We should examine whether information gathered by the operator is covered by the Act, since the monitoring is not performed while the conversation is taking place. We can use an analogy to the Internet, as the ISP transfers data but not while the conversation is taking place. Sending an SMS as part of the localized services is also handled by the PPA, under section 17F(a), which provides that any direct mailing should include a clear message indicating the registration number of the database used, the right to be removed from it, the identity if its owner and the sources from which he received this information. Of course the application of the Act is linked to the type of information concerned, and it is doubtful whether geographical information is part of a conversation. The Secret Monitoring Act protects the contents of the conversation.

Unjust Enrichment Act of 1971. It may be that transferring the information to a third party for pay without the cc of the user constitutes a breach of this Act a preliminary question or to whom the information belongs: to the use or to the collector? The answer is based among other things on the determination on the right to privacy, and thus we enter a magic circle.

Private or Public Regulation?
There is no doubt that the PPA was enacted in view of a technological reality that was different form today's. There is no doubt that this arrangement needs to be updated, especially in light of an information age in which we live in the past decades. When

\textsuperscript{356} Appeal 86/89 State of Israel v. Bank Ha'Po'alim, 44(2) P.D. 726.

\textsuperscript{357} Netvision v IDF (unpublished).
we argue for the need to create a new public legislative arrangement in a certain area, we should remember that such a step may have various negative costs: first, the legislation costs can make the use of the cellular networks more expensive, after it has become a "basic product" in any household in Israel. Therefore the costs should not be externalized at the expense of the users. Secondly, we should consider the timing of such regulation, the mobile filed is dynamic and some argue that the revolution has not reached its pick yet, as the cellular Internet is a revolutionary product. As we have seen the legislation in the U.S. did not wait for the technological developments and enacted the USA PATRIOT Act after the September 11 events.

However, a law enacted before the nature of the developments in the field becomes clear may restrict the discretion of the court to an excessive extent. Frequent amendments of the law may compromise legal certainty. Thirdly, the field of geographical localization has confidential uses and is therefore not publicized. Public regulation can act as a double edged sword as it puts the issue on the public agenda and at the same time the gap between the citizen and "big brother" grows even deeper. In view of these considerations, we shall examine the alternative of self regulation by the cellular market, by the operators or by creative technological solutions.

**General consideration regarding private regulation**

As we have seen in the U.S. there is a model combining public and private regulation. The American industry does not deal with privacy issues for altruistic reasons. It knows clearly that if it does not act upon its own initiative, the government will pass legislation to regulate this subject. The success of this model is partly due to the strength of consumer culture in the U.S., operating self means such as consumer boycott where needed.

---


361 In 1999, Pentium announced that the new process (Pentium 3) will include a serial number (PSN) to identify users in electronic transactions. Following a boycott against it by consumer organizations in the US, this technology was not used. See: Haim Ravia, *Privacy on the Internet (Part 3)* http://www.law.co.il/showarticles.php?d=h&article=46 (Hebrew)
C. **Possible Solutions**

C.1. Private Regulation

In the first chapter we presented the types of regulation. Here we shall focus on the means of surveillance described above. Private regulation in this context means that the individuals, rather than the state, regulate - among themselves and on a unilateral basis - the ethical problems of violation of privacy. These individuals may belong to one of two groups: the end-users or third parties.

1) **The End-Users**

The end-users see themselves as the direct or indirect victims of the violation of privacy as a result of means of surveillance. Internet users belong in this group. This is the conclusion of the previous sections, since it is not possible to surf the Internet without being constantly exposed to the dos. Moreover, as we shall see in the next section, often the current laws cannot aid the users whose privacy is violated. It is also known that not anything that is legal necessarily is "kosher" in terms of its effects on society, in the same way that not every act that conforms to social norms in a certain community is legal. The end-users can choose between three main courses of action in order to handle such violations of their privacy: technological means, trust in the market forces or a code of ethics.

1. **Technological Means**

In the previous chapter we presented the various technological means with which the end-user can handle the constant threat to privacy and property caused by the means of surveillance. Among these are programs, fire walls, external routers and VPN based technology, changing the default preferences, side verification mechanisms (personal computer or local system passwords, ID and electronic verification, automatic redial, personal identification tokens etc. Following is a discussion of three other technological means: encryption, P3P and Anonymizer.

**Encryption and Digital Signatures**: these almost completely prevent the monitoring of electronic communication, such as e-mail, IRC (Chat) and ICQ. In

---

362 Another question is whether we wish to use legislation in order to handle these problems, with which we deal in the next sub chapter.

363 Eli Salzberger, "The Profession, the Ethical and What's Beyond the Law" 5 L. & Gov. in Israel (2000) 409, 412-413 (Hebrew).

general, electronic communications can be secured in one of two ways: first, physically securing the communication channel itself by establishing a unique physical communication line between two points. Point to Point and VPN systems are based on this technology, used by large companies and organizations such as banks, in order to create a system that cannot be accessed by the general public. The other option is to secure the information transferred through the network after it leaves the domain of its sender until it is received by the recipient, using encryption of the information transferred. The encryption programs are based on algorithms including mathematical functions, which can easily be calculated on one direction, but are very hard and sometimes impossible to solve in the other direction. In order to do so, the recipient should have access to the correct algorithm or be able to break the code by use of very powerful computers, that the average person does not have and since breaking the code with violence is not practical, the only way is to access the correct algorithm.

This approach is implemented in several ways, according to the types of encryption. We should distinguish between symmetrical encryption, in which the encryption key and the decoding key are identical and asymmetrical encryption, in which the encryption key is different from the decoding key. By this concise explanation, it is clear that symmetrical encryption is not as useful online as asymmetrical encryption, as they require the sender to meet the recipient and give him the keys. Where the parties never met and are not likely to meet and the only connection between them is supposed to take place through the network - this raises a problem. Another option for transferring the key is sending it online, but a third party can monitor this transmission.

In a Public Key Infrastructure system, asymmetrical encryption is used, composed of a public key distributed among the recipients and a single private key held by the sender, there is a mathematical connection be the two keys, based on an irreversible function, when each private key is a larger prime number and the odds

365 Bar-Sadeh, at 246.
366 Supra note 184.
367 The tries to crack the code by trying a series of random codes. Ibid, at 18.
369 Bar-Sadeh, at 252.
that two senders could have the same key is close to zero. The sender uses the public key in order to encrypt the message sent and then the private key in order to decode the reply. The advantage of this method is clear - even if one of the public keys is discovered by the "enemy", he cannot use it to encode the message sent, and the parties don't have to share one symmetrical key and constantly secure it.

The digital electronic era made the traditional signature no longer a sufficient means of proving that the sender signed a certain message, to verify that the person who claims to be the sender is indeed the person who sent it, and that the message received by the recipient is the same one that was sent by the sender. The reason is that these days the traditional signatures can be forged easily and with surprising precision using the existing digital means. Therefore there was a need to create a parallel signature - the digital signature. To create a digital signature asymmetrical encryption is used, the sender signs the message using a unique combination of letters and numbers, encrypts it using his private key and the recipient decodes the signature using his public key.

The use of digital signature has many advantages: it creates a significant difficulty to those who wish to forge it, due to the asymmetrical encryption; the original document sent is identical to the one the recipient received, as it cannot be altered without the sender's knowledge; third parties can rely on the message, which enables the transfer of documents such as checks; and finally, certainty. Based on the technical infrastructure described above, it is clear that the sender cannot claim that he was not the person who signed a document carrying a digital signature.

However, the disadvantages cannot be disregarded: firstly, the cost of these advanced technologies, constantly developing in order to create new harder to decode algorithms, as the counter measures are always developing. Another problem is the fear that hostile parties may use it against the state. It is also feared the third parties

370 Kozolovski, at 332.
371 Ibid.
372 Bar-Sadeh, at 253 and Kozolovski at 336, 331.
373 Kozolovski, at 336-337.
374 Therefore, for example in the U.S. encryption technology is considered a military weapon, requiring a special license. In the UK the Regulation of Investigatory Powers Act 2000 allows the authorities to inspect e-mail messages and encrypted transmissions on the internet and the ISPs are obliged to assist them. In Israel encryption technology is under supervision under the Supervision of Products and Service Act1957. See Bar-Sadeh, at 256 and The Fighting Terror Online, supra note 63.
may decode the algorithm or invade the sender's database and use the digital signature in his name. Such a scenario renders useless all the advantages described above.\(^{375}\) The Israeli legislator as aware of this and enacted in 1992 the Electronic Signature Act, granting normative validity to digital signatures.\(^{376}\) Section 2 of the act provides that under certain conditions there is a presumption that the electronic (digital) signature is equivalent to as a physical signature.\(^{377}\) Similar acts have been enacted in may other countries.\(^{378}\)

**The Platform for Privacy Preferences Project (P3P)** is a technology standard created by the W3C (World Wide Web Consortium), with the purpose of providing the end-users with a means to gain further control of the personal information gathered by cookies. This platform, now installed in the latest version of Internet Explorer (IE6), give the use the option to choose the level of invasion to his privacy he is willing to accept and to compare it to the level of privacy violation on every sites he visits.\(^{379}\) On the basic level, P3P is a series of multi choice questions covering some of the aspects of the privacy policy adopted by the sites. Answering these questions creates a general picture about the question of how the site concerned handles the personal information gathered on the visitors. A site that supports P3P allows for this general picture to be compiled into XML format, that the browser can read automatically and compare them to the privacy preferences chosen by the end-user.\(^{380}\)

The problem is that technically the end-user has no ability of knowing the significance of choosing, for example, a "medium" level of privacy, as he did not design the standard himself. Also, the site defines its own level of privacy. In addition, there are many end users who still are not aware of the standard and how to use it.

Anonymity sites. There are several sites on the Internet that are used as

\(^{375}\) Kozolovski, at 317-318


\(^{377}\) In order for the electronic signature to be considered an "ordinary" signature, it must be verified. Under section 1 of the Act a certificate of verification should be issued. In addition, the signature must be secure.

\(^{378}\) For example the Electronic Signatures in Global and National Commerce Act, 2000 in the US and similar laws in Germany and some other EU member states.

\(^{379}\) Technically, this is done through the Internet Options.

\(^{380}\) [http://www.w3.org/P3P/#what](http://www.w3.org/P3P/#what).
mediators between the end-users who use them and other sites that wish to gather information. The most prominent among these is anonymizer.com, that provides anonymous surfing services to any site, the destination site is unable to gather information on the user. Another site is hushmail.com, through which the user can send and receive encrypted e-mail. The messages and attachments are encrypted before they are sent from the sender's computer and until they are received by the recipient's computer, where they are automatically decoded (end-to-end encryption). The site operators claim that this method guarantees maximal privacy, even against the "Carnivore" FBI sniffer. Another site is junkbusters.com, where end users can download a program to help them delete cookies and adware (pop up windows). However, the difficulty arises since the user should be able to trust a third party providing the "smoke screen".

2. The Market Forces

This course of action is concerned with the economic aspects of the web and their derivatives. It is possible to contact certain advertising companies and inform them about their sub contractors' use of harmful advertising tactics. It may be that in some cases respectable companies may not want their reputation to be damaged due to privacy violations.\footnote{Advertising.com stopped working with C2 Media after learning from a PC World reporter of its methods. See: \url{http://www.sitepoint.com/print/888}.}

However, this course of action is not always efficient, due to market failures. For example, there is a significant information failure on the web, as a result of which, among other things, not all end-users (to use an understatement) know which sites and which companies violate their privacy. Even those users that have the information are not always willing to invest efforts in campaigning against those companies, as they wait for someone else to do it for them (the free rider problem), and since they believe that the struggle against large and wealthy companies is a lost one. As a result, if the media publicizes the information failures, this may lead to success between the number of vulnerable users and the difficulties in organizing them prevent reliance on this course of action.
3. A Code of Ethics

We see the Internet as an old-new culture, renewing many aspects of the general human culture as we know it, and its basis is parallel to the physical reality. Therefore, in general, ethical rules, namely the unwritten criteria that determine what is ethical, should apply in the digital environment. However, they should apply in accordance with the unique architecture of the web and its effect on common human behavior.\footnote{See also Naama Carmi, a lecture given at the Computers and Education Conference June 27, 2000: \url{http://www.notes.co.il/carmi/324.asp?p=2}.}

One of the main changes is the fact that there is great intimacy on the web, resulting from anonymity, as when a person surfs the web he feels free to take off the "masks" and protection mechanisms, the products of modern capitalist society. The Internet society encourages this as it leads to the realization of values and rights which in the real physical world cannot be realized. On the Internet no one is rich or poor, Muslim or Jewish (unless, of course, the users want these distinctions, made out of choice).

This is the positive aspect of intimacy on the web. The less positive aspect is the fact that many users exploit this intimacy in order to act against other users, as described in the previous chapter. Many users and commercial bodies that would not have dared to break into other people's homes or tap them, do similar acts on the web for their persona or commercial purposes. They succeed in doing too often due to the failure of enforcement on the web, resulting from online anonymity, the structure of the web, and the advantages of knowledge, which we shall now discuss.

The second main difference between the digital environment and the physical environment, relevant to the matter at hand, is the differences in knowledge between trained users and certain commercial bodies and between most amateur users. Unlike the physical world, in which staying for a few months in one place is sufficient n order to learn the local customs, in the digital environment the learning process never ends. On the one hand, the sources of information on the web are endless.\footnote{Gabriel Solomon \textit{Technology and Education in the Information Age} (2000), 35 (Hebrew).} On the other hand, not all users are able or willing to invest time in acquiring the knowledge to help tem fight against the violation of their privacy. Even if the average user learns about the solutions it does not mean that he can afford them, due to the endless "arms
race". Furthermore, it is not clear that the Internet community would be interested that the body having the greatest potential of enforcing norms of appropriate behavior online, namely the state, should be the one to determine what may or may not be done. Firstly, because this is likely to reduce the freedom of users and secondly due to the constant fear of surveillance by "big brother". Another reason is that, as already noted, the law cannot always help and does not necessarily provide the best solutions.

(2) Third Parties
This group includes all parties that are not end-users, but have a significant connection with this issue. They can be divided into two sub-groups: For profit entities: mostly private companies engaged in developing technologies or tools for privacy protection. On the face of it, it seems to be a natural solution: the market forces respond to the demand for toll to protect privacy and supply various solutions. But there are problems that are inherent to the private market, in particular conflict of interests. The companies have an interest in offering solutions to the end users, but they do not have an interest in ending this phenomenon, and thus it is a short way from developing means of protection to developing means of surveillance.

Another example is the site owners themselves, who often present a privacy policy in which they undertake not to violate the privacy of their visitors. However, often these policies amount to misrepresentations and in practice those site do indeed violate the privacy of their visitors. Not only that but in many cases the user would not be able to find the privacy policy easily, and even when he finds it he may not find an explicit undertaking not to violate his privacy. Other bodies, such as internet advertising companies, have a clear conflict of interest between their undertaking not to violate privacy and their ongoing activities.

Another problem of the private market is that the companies operating in it are the product of private initiative and can therefore compromise the users' privacy in order to become more efficient or profitable, which may cause the costs or damage to be born by the consumer.

Non profit bodies - different bodies having ideological, altruist, educational or

384 E.g., the Echelon Project
social motives may try to protect privacy. Unfortunately there are very few bodies in this group. The prominent one is W3C that created the P3P among other things. Another organization is EFF (Electronic Frontier Foundation), a private organization funded by donations, with the purpose of "protecting out basic rights to think, speak and share out ideas, thoughts and needs by using new technologies such as the Internet." The basic right this organization seeks to protect is the freedom of speech. Another prominent organization in this area is EPIC (Elementary Privacy Information Center), a research center based in Washington, with the purpose of putting on important topics the public agenda, relating to basic rights, including the right to privacy and various constitutional values. This organization is also by donations and is not subject to any American governmental authority.

The main problem with bodies like these is that most of their members are technology people who are not necessarily knowledgeable of the normative questions on privacy on the Internet. Even when we deal with organizations that engage in questions of value as a direct and central part of their activities, they cannot be said to represent the majority of the Internet community, as the rest of the end-user s do not identify with their positions and would not appoint them to decide which values should be represented by technology. Moreover, these bodies are not appointed by an authority, but operate out of a sense of mission and commitment to the cause. The result is that as although these organizations are a positive phenomenon, they are not subject to any rules or principle, legal or otherwise and are not accountable.

An interim venture is collaborating of the industry and non profit organizations, for example the TrustE organization, which is a union of many sites that accept its privacy policy and display its logo proudly on the homepages. The advantages of this course of action are clear - all the end user has to do is search for the organization's seal of privacy and once found - he knows that the site is committed to a certain privacy policy. The member site enjoys reputation and reliability. The main problem is the constant conflict of interests between the organization and the member sites. However, in practice, the companies heading the organization and those that are

385 http://www.eff.org/about/.
386 This organization acted on the activities of the secret services in the E911 affair, where a document was copied unlawfully from the computers of Bellsouth, detailing the operation of the 911 emergency line.
387 http://www.epic.org/epic/about.html.
members in it are the same ones.

**C.2. Public Regulation**

Where a basic right is threatened or where there is a market failure and there is a fear that private regulation would not provide efficient solution for it, the option of public regulation should be considered. When it comes to new technologies, there is a fear of legislative intervention that may hinder technological progress. However, the greater the threats and its damage, the more important it becomes to consider legislative regulation. We shall discuss the subject and specific issues, as well as a comparison with other countries.

(1) **Internet Service Providers** (ISPs) - in the U.S. the Electronic Communication Privacy Act (ECPA) was enacted in 1986.\(^{388}\) In the part relevant to the matter at hand, the Act forbids an ISP to invade the e-mail communications on its systems, change them or block the recipient from receiving them. One of the purposes of this Act was to create uniformity in the law applying to the various electronic means of communication (telephone, modem, E-mail, fax etc.). The Act is vague, for example in the provisions authorizing ISPs to monitor emails by end users. The broad interpretation of these provisions would maintain that the ISP may monitor emails whenever there is a fear of defamation or criminal offences. Adv. Jonathan Bar-Sadeh expressed the opinion, which we support, that the e-mail messages are not comparable to contents on websites (for example in chat rooms), and therefore the provisions should be interested narrowly with regard to the freedom of ISPs to invade the users' privacy.\(^{389}\) The reason for this is that e-mail is similar to ordinary mail. A mailman cannot open out letter to see of they contain problematic materials, and similarly the ISPs should act in the same way. Moreover, when the end user presents his materials on a webpage, he is not entitled to expect privacy, but when he sends a mgs through e-mail, he does have this expectation.\(^{390}\)

(2) **Hostile Parties (Hackers).** Despite the common belief that hackers only cause

\(^{388}\) Electronic Communications Privacy Act 1986 18 USC §2511.

\(^{389}\) Bar-Sadeh, at 281.

damage, in practice this is often not the case. Hackers assist in testing the efficiency of information systems and check for security loopholes. However, this cannot exempt them from responsibility for their other sins, and the bottom line shows that the damage they cause is greater than the benefit. When a hacker sends a Trojan horse into the end user's computer and causes damage, clearly this hacker, if caught, is liable under civil law, usually under a tort. The problem arises when no physical damage is caused and the only damage is the violation of the right to privacy. From a normative perspective, one of the purposes of this document is to show that the right to privacy stands in its own right and consequently a remedy should be granted for its violation, regardless of whether or not any economic damage or damage to property were caused during the violation or as a result of it. In the past, information was a means to the purpose of committing an offence (usually gaining physical property), whereas today obtaining the information itself is the incentive for the offence. However, although the privacy laws often apply to invasion into one's computer, the applicable laws are different where the attacker is exposed to the end-user's private materials. In the case of invasion to privacy the PPAs apply whereas in the case of invasion into a computer the relevant laws are the Computer Act and Secret Monitoring Act.

**Computer Act and Secret Monitoring Act.** The legal battle against privacy invasion through means of surveillance is fought both in the criminal and civil arena. In general, the criminal offences in this field are based on the parallel offences in the physical world, mutatis mutandis, in particular fraud, theft and forgery. The offences created in the past few years are intended to give an urgent reply to the problem of the inability to enforce the physical law in the Internet world, due to the unbridgeable difference between the act done and the relevant physical offence. These offences can be divided into three main areas: theft and destruction of online

---

391 Bar-Sadeh, at 692. In practice the courts seldom consider the positive activities of hackers, see CF (Jerusalem) 3813/99 The State of Israel v. Oded Refaeli, Takdin Supr. 2000(2), 1091.
392 See chapter 1A.
393 Bar-Sadeh, at 670-671.
394 Answering this question requires a review of the interpretation of the right to privacy, see Chapter 1.
395 Bar-Sadeh, at 669.
396 Bar-Sadeh, at 672-682.
electronic information, including unauthorized entry into a computer system, trespassing, unauthorized use of a computer and changing or damaging data. These acts, as explained in the chapter on means of surveillance, are done whenever a means of surveillance is used. As noted, the relevant legislation in this field does not emphasize the pure economic loss caused to the end user, but erects a virtual fence around the computer systems and the information they contain and determined that whoever attempts to trespass is considered as having broken into real property, and thus the law views him as an offender. Without these legal provisions it would not be possible to enforce the law on the Internet. However, in order not to extend criminal responsibility excessively, the legislator determined that the invasion should be unauthorized. Yet, as Bar-Sadeh notes, it is important that the requirement of authorization applies only in appropriate cases, and considering the structure of the web, its nature and its purposes, as opposed to, for example, a situation where a user innocently enters an open unrestricted system. The responsibility is further narrowed down by use of sections that include "close lists" of conduct viewed as an offence. However it should be noted that the view that sees the computer as "property" and therefore considers the invasion damage to property is controversial. Another area is the offences including causing damage, destruction or altering electronic data. These can be used against hackers who invade computer systems in order to destroy them. The objective is to create commercial certainty - society wished the information to be available, reliable and complete. In Israel section 6 of the Computer Act establishes an offence that forbids the development of computer viruses, transfer them or plant them in another person's computer with the intent of causing unlawful damage or disruption to the computer or to materials on it. In the case of Gill Paz, six month imprisonment was sentenced for infringing section 6 of

397 Bar-Sadeh, at 674. See for example section 4 of the Computer Act 1995, which does not include among the element of the offence of invading computer materials any cause of damage, but assumes tat the invasion suffices.

398 For example in the Computer Act the phrase "unlawfully" is often used (e.g. sections 4-5).

399 Bar-Sadeh, at 674-675.

400 Bar-Sadeh considers that in the context of stealing information, unauthorized use or copy should be included as depriving the owner of the information although it is left in the hands of its owner. The information is the protected asset such use of it dilutes its value.

401 Cf. section 2 of the Computer Act.

the Computer Act. It was held that section 6, despite its title ("Computer Virus" applies also to other types of malicious programs, including Trojan horses. However, in our opinion a distinction should be made between Trojan horses and computer viruses and between other means of surveillance, since the damage caused by the latter is less severe than that caused by the former. Another reason for his distinction is the many positive uses that can be made of the other means of surveillance, as described in the previous sub chapter.

The final area of computer crime is unauthorized access or use of electronic information systems. Unlike the other two areas, here the offence requires intent or knowledge that the access is unauthorized. In Israel this is covered by section 4 of the Computer Act dealing with unlawful intrusion into a computer, with the exception of cases covered by the Secret Monitoring Act, in which the monitoring is passive and does not involve actual invasion. Therefore the Secret Monitoring Act applies, for example, to the use of sniffers or monitoring e-mail messages, but not to spyware or cookies. In the U.S. the Computer Fraud and Abuse Act of 1984 deals mainly with unauthorized access. In 1994 the law significantly amended and applied also to the Internet, forbidding criminal use of computer systems. In the case of United States v. Morris a virus was planted in a computer network, and it was held that the mens rea required for the offence is the intent to invade into the computer, rather than the intent to cause damage. A different conclusion is drawn from the provisions of the Israel Computer Act, section 2-4 in particular, where there is no requirement for mens rea and thus no need to prove criminal intent. Obviously the general part of the Criminal Act applies here.

Beyond the said criminal legislation, the Computer Act provides in section 7 that unlawful interruption with the use of a computer or computer materials as well as deletion of such materials, altering them or disrupting them constitute torts. Under section 9 the mental element for this torts is at least negligence, otherwise no damages can be awarded.

An end-user harmed by the invasion into his privacy sue to the use of means of


\[404\] United States v. Morris, 928 F.2d 504 (2d Cir. 1991).
surveillance can rely on other torts, such as trespass, negligence, fraud etc.\textsuperscript{405} as well as contract law, unjust enrichment law and intellectual property law (breach of trade secret, copyright etc.) however, the remedies, if awarded, are often awarded only for physical damage or unlawful use of the information, rather than the violation of privacy. The end-user can rely on the general law only where the invader was under a duty under the law of tort\textsuperscript{406} or the law of contracts\textsuperscript{407} not to violate his privacy. This question is linked to the general conceptual problem of the term "privacy" discussed earlier in this paper.

**PPA.** Of the list of conducts forming privacy violations under section 2 of the PPA, three are relevant to the matter at hand. Firstly, section 2(1), prohibiting spying or following a person in a manner that may harass him or other types of harassment. Cookies, spyware, Trojan horses and sniffers can be covered by this section. Yet this section was narrowly construed in the case of \textit{Vaknin}. Section 2(2) deals with prohibited monitoring and applies the provisions of the Secret Monitoring Act to situations where the passive monitoring of one's actions cause violation of privacy. Another relevant section is 2(5), which prohibits copying the contents of a letter or other written document not intended for publication without the permission of the recipient or the author. This prohibition can cover emails, but this requires legal interpretation that cannot be taken for granted. The infringement of these provisions is also a civil tort under the Tort Ordinance well as a criminal offence.\textsuperscript{408}

The main problem of the PPA is that the legislator clearly did not foresee its application to the digital environment. Sometimes the provisions can be applied through interpretation to new situation, but this is not always easy. It is possible to amend the Act, but it is doubtful whether technology-dependent technology is desirable, which may soon become irrelevant and hinder technological developments.

\textsuperscript{405} Section 63, 56, 36, 35, 31 of the Tort Ordinance.

\textsuperscript{406} For example where a program was not presented as spyware while in fact it was.

\textsuperscript{407} For example, an operator that declared that it does not use cookies but in fact did so.

\textsuperscript{408} See sections 4, 5, 29 of the PPA.
D. Conclusions

In view of the aforesaid, many consider that the following conclusion is inevitable: "You have zero privacy anyway, get over it."\(^{409}\) We think differently. We maintain that although the race between law and technology will never end, and at the moment technology is winning, there is no need to surrender the values we think ought to be protected on the Internet. Yet clearly the means of surveillance should not be treated as a single group. The distinction presented at the beginning of this chapter is also relevant to our conclusions:

1. One group includes means of surveillance aimed mostly at monitoring the activity of the end users and have no other use which is not negligible compared to the harm the cause (spyware, Trojan horses, Internet bugs and various spyware programs that can be easily obtained on the web). Their social value is relatively low, the cost of fighting them by technological solutions is high ands the damage they cause can very substantial. Therefore we consider that private regulation is insufficient and public regulation ought to be used. The current legislation should be amended, as explained above.

2. The legislation should, in our view, obtain two main objectives: disclosure and consent. Whoever wishes to violate one's privacy using the means of surveillance belonging to this group, should inform the user in a manner that is clear and understandable by the reasonable user and obtain his full, explicit consent. In other words, the duty to inform users should be strengthened and extended, and the consent should be clear. On this issue we support the Ministry of Justice memorandum, which suggests a level of "informed consent" imposed on the web.

2. A second group includes means that have other uses, not having peripheral significance compared to the damage they cause (cookies, sniffers and cellular phones). In general terms, with regard to this group of means of surveillance, private regulation solutions are called for, including a code of ethics, recruiting the market forces and using technological solutions and standards that are different to those of commercial bodies or non profit organizations. The reason for this is simple. If we

---

\(^{409}\) Scott McNealy CEO, Sun Microsystems Comments to reporters at an event to launch Sun’s Jini January 1999.
requires that the various bodies that use such means of surveillance to be subject to the same rules and criteria as the ones imposed on those using the means of surveillance included in the first group - this may lead to paralyzing the activity on the web, and to the disappearance of many features that make it unique compared to other media. For example if we demand that each website ask for an express approval to use cookies from each visitor, surfing would become significantly more cumbersome ad the web less popular. This is true with regard to cellular phones too, which are used in our everyday lives and the surveillance is only a tin part of their use. With regard to sniffers one may say that they have many positive uses for various parties, weighing more than their negative features.

Legislation is another possible solution, to ensure that the borderline between the beneficial use, usually forming an integral part of the technology - and the use causing a violation of privacy is maintained. For example, legislation to ensure that the cellular phone companies do not use the geographical information created during use of a cellular phone for marketing purposes, unless the user gives her express consent to such use. To a certain extent, this is the legal situation today, based on section 2(9) of the PPA and the requirement of consent in section 1 of the Act.
3. **Databases**

A. **Introduction: The Information Chain**

The database is in the center of an information chain, composed of parties and actions. This chapter discusses the various links in the chain. A simple information chain is a communication system comprising only two parties. Information passes from the first party that holds the information to a second party. The first party is the information source and the second party is the destination. The actions performed are transfer by the first party and receipt by the second. This chapter describes an interim party. After the receipt from the source, it performs the actions of collection and storing. Then it uses the information itself or gives it to a different destination. In the information chain we are dealing with, the interim party holds the database. Another party in the information chain is the mediating tools used by the bodies with which they perform actions using the information. Here we deal with tools based on computer systems.

The source of information is often the person to whom the information relates. Yet there are cases in which the source is a different party holding such information. A simple example is one's name and ID number. These are registered (in Israel) in the national registry by the parents, after birth. In other cases, after a person provides information that is later held in a database, the database or its owner can serve as a source in the information chain and start new chains, and so on.

When a person provides information he or she may or may not consent to doing so, the destination can use means of surveillance in order to gather the information, unknown to the source. When dealing with computers and the Internet, the information will be gathered in a database. The interim party is the database owner. Holding the information in itself is an action, but the information can then be transferred to another destination. Furthermore, many uses can be made of the database, such as running a sophisticated spam system. The person in the scenario just described turns into an entry in the database. This person or any other party on which information is gathered are called *data subjects*, a term reflecting the status and power within the information chain, that person is indeed a subject in our view.

**What is a Database?**

In technological terms, a database is a collection of data of various types, stored in one or more places, under certain rules or with no rules. The data can be sorted in
different ways. Therefore a sentence, a paragraph or a single dictionary definition are not databases, and neither are literary or musical creations. A database can be assembled from any collection of contents and can have fairly wide definitions.

Databases have several clear advantages. They enable the storage of large amounts of data, locate and retrieve it with ease and flexibility, search in accordance with several criteria (not only one rigid criterion) or find patterns within the data. They are easy to use and make it possible to distribute the data with relative ease.

<table>
<thead>
<tr>
<th>Digital Information vs. Printed Information</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Accessibility</strong>: digital information arrives everywhere through websites, e-mail and so on; the number of copies is the number of consumers.</td>
</tr>
<tr>
<td><strong>Availability</strong>: digital information is available at any time.</td>
</tr>
<tr>
<td><strong>Contents</strong>: digital information contains, beyond text and graphics also images, sound, animation, video etc.</td>
</tr>
<tr>
<td>Digital information is <strong>up to date</strong> (new developments in science and technology, information on current affairs around the world, information published by companies etc.)</td>
</tr>
<tr>
<td><strong>Dynamic</strong>: digital information is dynamic and constantly changing (whether reports, satellite images, news etc)</td>
</tr>
<tr>
<td><strong>Searching and retrieval of information</strong>: digital information can be easily retrieval using digital search engines.</td>
</tr>
<tr>
<td><strong>Saving information</strong>: digital information is easy to save and publish</td>
</tr>
<tr>
<td><strong>Verifying information</strong>: this is problematic, as anyone can publish anything and it is sometimes hard to identify the source of information and to evaluate its reliability. However there are quality and up to date databases by academic and/or educations bodies.</td>
</tr>
</tbody>
</table>

**Technological Developments**

The important technology developments include a significant reduction of the storage costs and the cost of processing information. The ability to store and process information has improved over the years from a technological point of view, so in fact it is possible to obtain quality technology at low prices, at least for some parts of the

---

public and certainly for large organizations. These changes can be defined as deriving from the essence of the digital means that have created an ability to form large complex databases and yet decentralized on computer networks and use of expert systems for processing.

As a result of these new uses, the way in which information is processed and analyzed has changed and alongside the permanence of digital information, these create a digital environment that has more information than we could imagine in the past, the information is accurate and can be cross processes due to its availability and in particular due to the wish of the state and the private organizations that can benefit from it.

The important features of databases in our opinion is the ability to collect and store large amounts of diversified information and link them, so that each piece of data from one area can lead directly to data from another area. But in this chapter we shall argue that these features led to loss of control over the data by the database owner and the data subject and the user has almost unrestricted access, which leads to violation of the data subject's privacy.

The term database becomes vague in view of the decrease in the importance of the geographical aspect and the ability to control it from a distance through computer communication. They are not necessarily located in the same physical location, but are built and disappear dynamically and can be accessed and controlled from distance, and in addition their strength is constantly improving and they are all accessible to the public. These facts increase the possibilities and advantages of databases, but at the same time the fears arising from the problems they create. The next section discusses the dangers and problems and dangers of databases.

**Computer Databases - Technological comments and Basic Terminology**

1. *File* - a collection of interrelated data items.

2. *Record* - information relating to a person, a product or an event.

3. *Field* - any item included in a record is a field. For example, a library record includes several fields: the author, the book title, the year of publication etc.)

---

411 Recognition of the value of data analysis led to the establishment of companies specializing in data mining and in analysis and evaluation of info through cross processing. The development of methods for organizing and marketing knowledge is in fact an economic branch.
4. **File management** - the records can be updated (adding, deleting and changing the information), verified and secured (preventing loss of information or unauthorized access).

5. **Sorting information** - usually by reorganizing the records according to certain criteria. Databases use programs for running databases that sorts the data.

6. Basic operations:
   - **Search**: database systems allow for flexible searches. The program performs the search as a series of decisions
   - **Inquiries**: action the allow search of a record or all records that answer certain criteria.
   - **Data mining**: an attempt to find links between data items that are unpredictable or unknown.

(1) Database Modules

- **Relational** - the fields of each record are organized as a series of boards containing rows and columns. Each of these is a "flat file", a simple database including one board with rows and columns containing information.

- **Hierarchical** - operates like a family tree.

- **Network** - a collection of data focus and a large number of links connecting them

- **Object Oriented Database** - a networked database that can link different types of data such as text, graphics, images, sound and video and can link them to a certain object.

**B. The Dangers**

What are the dangers and problems created by databases? Why should we doubt the need to exploit their advantages as much as possible? This section has three parts: in the first part we lay the foundations for the theoretical perception of the dangers to privacy, in the context of databases. The common perception, we argue, is based on clear narrative foundations, but these are insufficient in order to understand the full picture. We suggest additional foundation to complete the existing ones. In the second part we discuss in detail the phenomenon of databases and present tools for distinguishing between different types of databases, using the terminology described above (the information chain). In the third part we prepare a summary of the dangers and problems of databases and the differences between them. We shall use this summary when we discuss the regulation of databases.
B.1. Theoretical Introduction - Big Brother and Citizen K

The legal models of privacy protection are designed to protect against feared violations, based on a certain perception. An incorrect perception of the fears and the threats leads to incorrect conclusions about the privacy protected by the law and the interpretation of the concept of privacy. We present the suitable perceptive frameworks, in our view, in relation to databases. Professor Daniel Solove's article on the narrative analysis will assist us.

Professor Solove draws a distinction between the common perception of the threat of databases, the fear of "big brother". He presents this view and argues that it is wrong or at least insufficient in order to understand reality. That famous phrase by George Orwell is normally attributed to the state, but in the reality we live in there are "little brothers", or "private brothers" that form a substantial factor in our lives. These are the private sector bodies that maintain private databases. Solove argues that the real, imminent threat is not by the state, but by those privately owned bodies. The lack of regulation in the digital environment will undoubtedly lead to "Orwellian" results, mainly due to the threat of the private corporate market. When private forces rule the market there is a fear that the lack of supervision (legislative, legal etc) may allow them to exploit their economic power in order to gain access and control of information and use them in illegitimate ways.

The Orwellian view of privacy focuses on the fear of invasion to the private domain, gathering personal data and intimate information. This view is especially suitable to describe the violation of privacy on the Internet, while the information is gathered and before it is stored. This describes the problems caused by the means of surveillance and the problem of consent, described in the previous chapters.

Another view is the Kafkaesque perception of the problem of privacy, referring to the lack of control over information and processes related to it. This reality is described in terms of bureaucracy, arbitrariness, inhumane treatment and lack of thought. As in the Kafkaesque "legal" system, any system that conducts its relations

414 Solove, at 1398.
415 Ibid, at 1418.
with people through databases stops treating them as human beings. The person cannot recognize and identify the factors and processes that affect him and matters are being conducted without him being able to understand or influence them.

The practical result of the Kafkaesque reality is complete reliance on the information contained in databases for every act and process in the market and in the social state. Since the database slowly becomes the basis for the conduct of any organization, we witness a risk of confusion between information and knowledge, and in fact, universal use of information instead of knowledge. In such a reality, a mistake or lack of information about one's qualifications, for example, turns into knowledge about his lack of qualifications. Furthermore, a problem of lack of control arises, the control that the database takes out of the hands of the data subject.

The problems of lack of control and the information turning into knowledge is evident from an Israeli case, where significant damage was caused to a new immigrant who was mistakenly filed as mentally ill and the information about him was registered by the Ministry of Interior. He found it difficult to find work and in most workplaces from which he was rejected he was not told the reason for this. The mistake was discovered only several years after the incorrect registration, and the Ministry of Interior claimed that the reason was similarity between his personal data and those of another person who was indeed mentally ill. This case demonstrates the strength of a mistake in processing information and the implications of lack of control and supervision when it is under the complete control of a public or private body.

B.2. Who Owns the Database?

1. Governmental Databases, Private Databases and the Flow of Information

In this sub chapter we shall rely on the distinction between the different bodies in the information chain. The information chain comprises a source, an interim body and a destination. The privacy laws were designed to protect the data subject. These terms will be used as a basis for the distinction, in order to classify databases, four relevant

---

417 Solove, at 1426.
418 *David Tazzezo v the Ministry of Health* (unpublished, 5 March 2005)
questions can be asked: firstly, who owns the database? Secondly, who is the source giving the information to the database or where was the information gathered? Thirdly, who is the destination of the information, namely, who has access to the database and uses it or to whom information from the database is given? Fourthly, and most important, who are the data subjects? We shall discuss the first question, regarding the database owner and ask the other questions in the course of this discussion. The question regarding the database owner has two possible answers: some databases are owned by the state and some are under private ownership.

2. Governmental Databases
The governmental databases are the product of the need for supervision of public interests. As the modern governmental system of supervision extended, the technology of databases and computer technology in general developed. In the U.S. the various federal arms as well as the states keep and maintain databases on their citizens, the number of databases is over 2000 in different areas. The databases contain information on immigration, bankruptcy, social insurance and so on.

States hold databases on arrests, birth, criminal record, marital status, ownership of property, voting, DNA and certain occupational licenses. In some cases the databases are published on the Internet, for example, the databases on criminals. The public aspect of governmental databases will not be discussed here, but we shall discuss in short the problems arising from their existence. The root of these problems is the way in which the information is gathered by the government, usually by coercion and not by consent. Sometime the information is gathered using means of surveillance, without the subject's knowledge. Usually the information is gathered legally for public purposes but where the government uses information from a private database, and where governmental information reached private hands, a problem arises (discussed below).

Another problem has to do with the transfer of information between public bodies, which was treated by the Supreme Court in the case of The Association for

---


421 Solove, at 1403.
Civil Rights in Israel v. The Ministry of Interior,422 in which the Court held that transferring data from the population registry to other public bodies, such as the Israeli Broadcast Authority is improper, as the recipient had no procedures or had insufficient procedures regarding the secrecy of the information, authorizing access to it and securing it. Following this decision many public bodies conducted comprehensive changes and changes in governing regulations are also foreseeable, initiated by the Ministry of Justice, that formed a committee to examine this issue.

Another problem is the growing use of outsourcing. The government uses private bodies that maintain the governmental databases. There is a fear that these bodies may misuse the information they hold. A main way to prevent this is to impose many duties on the private body in its contract with public body, and there remains a question as to whether legislative intervention is required.

Another difficulty arises due to the use of the information - its publication may infringe rights and interests. For example, in the U.S., Megan's Law, intended to serve as a warning against sexual offenders, impose a duty to publish their names and addresses, thus hindering their rehabilitation. As already noted we focus on private databases and wanted to indicate the difficulties with regard to governmental databases.

3. Privately Owned Databases

The imminent problems arising out of private databases refer to the use of the information and its destination. Processing information by a private body is normally for profit and not for the public interest, therefore it can be said to be suspicious even more than information gathering by the state. The suspicion usually arises in connection with the nature and the purposes of their general activities. The main fears are that improper considerations may guide the use of information, derived from the private objectives of the database owners. But there are also other fears, described below, related to the question of who is the source of the information in a privately owned database? The source can be the data subject, the government or other private bodies.

422 HCJ 8070/98 The Association for Civil Rights in Israel v. The Ministry of Interior, 48(8) P.D. 842.
4. The problem of public information in private databases

The databases common in the private market consist of information the source of which is the data subject himself. A simple example is a database kept by a service provider, where the data subject is a private client. The database contains information gathered directly from the client the problems arising in this context are mainly the issue of consent and means of surveillance. Other problems have to do with the use of the information and its destination.

We would like to present other common cases where the source of information is not the data subject himself. The first problem is the source. Where the source is the state, two scenarios can be described: information sold directly by the government to the owner of the private database or opening the public database for public access, and the private body can copy the information into his own database. After we present these scenarios we discuss the problems they create.

The first scenario is that of information sold directly by the government to the owner of the private database. The positive aspect is that sometimes there is a clear public need for use of the public information for instance for research purposes. The sale enables the state to have these needs answered by private bodies that can do so efficiently and even pay the state for the information. In general, it can be said that this activity may involve commercial consideration with those of the state that may overpower the necessary public consideration. Thus, a few years ago, the government of Iceland sold a database containing health information of the entire population for research purposes by private biotechnology companies. One of the arguments relating to this transaction was that the government gathered the information in order to sell it to that company, and did not act in the public interest, contrary to the Act that allowed this process. As already noted, such arguments are directed at the public aspect of the sale to private bodies, but we are focusing on the conduct of the private body that

423 For example in the 1970s the computer databases of the national census were sold to the private sector. Precautions were taken - the information was sold in small units with only addresses and no names, but within 5 years several companies bought a large number of units and cross processed the addresses with the entries in the phone books. See: Erik Larson, The Naked Consumer: How Our Private Lives Become Public Commodities 10 (Penguin, 1992).


425 See sites such as knowx.com, 441.co.il (active until recently), locateme.com, freepublicrecords.com.
maintains the database. We shall see how in the scenario just described, even legitimate use of the database can be suspicious, since the source is a public authority.

The second scenario, which is much more common, is granting public access to a governmental database, whether by personal application or through the Internet, for free or for a fee. Due to the easy access, a private body can use sophisticated means to gather information from the database and set up a new database based on the governmental one. Even when a fee is collected for access to the public information, the owner of the private database may invest money in purchasing it in order to sell it later for a higher price or in a more efficient manner. In most cases the database owner will not only copy the database, but will give it an added value before it is turned into a commercial service. In a most simple way the owner can create a database from public information that is not computerized or still has no distant access, and offer clients access through the Internet. The service will normally include information from several public databases. For example, the database copies from the land registrar enables immediate cross processing with the marriage register and additional databases. These options are not commonly given by the public administration today. This scenario led to public information being more accessible, open and efficient than ever and contributed to citizens' welfare.

There are many advantages to the public in the scenarios described and there are also problems relating to public administration. But as we shall now explain there are also problems arising in the relationship with the data subject and his privacy.

The first problem is that the rules applicable to those private bodies are not public law rules that apply to the public authority that gathered the information and published it. Gathering information and using it by the public authority are subject to public interests, but private bodies are not subject to such duties and can use the information for commercial purposes.

Another problem is the legal relationship between the database and the private

---

426 Other problems arise in this context, for example: it can be said that the scenarios we have presented indicate a digital environment facto privatization process of public services provided by the state. First, is such privatization being conducted in accordance with the appropriate rules ad discretion and should the service be privatized at all? Secondly, when public services are provided by the private sector, this creates a negative incentive for the public sector. From an economic perspective, there is no doubt that the sale of public information is economically beneficial, as the governmental funding invested in gathering the information continue to be invested in running the database, therefore the sale is a net profit transaction for the state. However, in the second scenario the state does not benefit, and it also looses the fees of those wishing to browse the information.
owner, which does not exist when it comes to the gathering of the information. As noted, in these situations the state gathers the information and the data subject is a citizen. Since gathering the information is usually legal, between the data subject and the database owner only the laws applicable to databases apply. Thus the data subject loses the variety of legal options relating to the stage of gathering information, which would normally be the main basis for claims against the database owner. The legal problem in these cases, in accordance with the Kafkaesque perception of privacy, is the individual's helplessness as against the private body that owns the database. The data subject has no clear claims against them, as they use information they are not responsible for. There is no opt-out option, since these are governmental databases.

5. The problem of information transfer within the private market

The source of the privately owned database can be another private body, including individuals and corporations. The transfer of information is the base on which the entire service and commodities market is run. Almost any company runs databases for the information used in its business. Basically, the information chain operates so that information is given by a client to the service provider who stores it in its databases. As part of the business relationship between the database owner and its suppliers, clients and other corporation, many information chains operate between them. Thus the information gathered from a client can be give to other destinations, and private corporations gather information from other corporations, the database market includes companies running sales and trade in databases fro billions of U.S. dollars each year. Companies selling products and service understood from the moment they started using databases as a routine, that they hold products of great value, and started selling the information. Other companies engage in this as their main activity.

This reality raises great fears for the privacy of the data subjects in the privately owned databases. If the information is known to be a commodity, this is most evident within the private market in corporate activity. This reality puts the privacy of the data subjects at risk.

427 We show this below when we discuss the legal models.
429 Solove, at 1408.
6. Transfer of information from private bodies to the government

This is the opposite situation of the first problem described above, as it arises where the private database is used as a source and the information is gathered by the government. This can be done in two easy: firstly, secret gathering of information using means of surveillance, but this is a matter concerning the conduct of public authorities, which we do not wish to focus on. Secondly, the information can be give voluntarily or by coercion. The state gathering information from a database formed by a service provider is a problem we will not discuss in depth in this paper. Yet as in the case of transfer of public information to private hands, this is an information chain, in which the source is not the data subject himself, but whoever gathered the information from him beforehand. As explained above, in these situations the claims the data subject has against the give are mostly in relation to keeping the information, while the gathering, that can usually base legal claims, is not a part of the relationships between them. It is important to note that a legal rule can solve this problem.

Such transfer of information between private bodies and the give occurs for different reasons, including the need for enforcement. We shall discuss the problem relating to the conduct of the private owner. It is similar to the opposite problem described above, namely the transfer of public information to private hands, but it may be argued that this case presents a more serious problem to the data subject. Where the information is given to the database owner by the data subject this is normally done as part of a service transaction and the information is given for the purpose of the service. In a contractual system, use of information beyond what is agreed upon constitutes a breach of contract and a violation of privacy. The state on the other hand can use the public information it holds in different ways within a very wide variety of relationships with its citizens. In his relationship with the private service provider, the reasonable expectation of the data subject is for a minimal use of the information, only for the purpose of the service agreed upon.

430 This also enables the state to evade many public duties. See the discussion below on American legislation regarding the USA PATRIOT Act.
B.3. The Dangers of Databases - Summary

Having discussed databases and their implications on a theoretical level, we shall now focus on specific problems. Reference shall be made to the potential uses of databases, especially their negative aspects. However, it should be noted that each of the dangers mentioned may have positive aspects that may be utilized by commercial bodies for example.431

1. Information Leaks

The digital environment and the web make it easy to access the information, including distant access. Information stored in a database may reach the wrong hands and maybe used for harmful activities or without the data subject's consent. The need for an appropriate level of privacy raises the problem of information security. Firstly, is it possible to completely secure information from exposure to unauthorized persons? Secondly, the information security policy selected has economic implications. It is possible have the consumers bear the costs on the, who in fact pay for the acts of a few.432

2. Data mining

Searching and gathering specific information from digital databases, for example, web pages, e-mail messages etc.

3. The problem of ownership

To whom does the information in the database belong? The data subject or the parties gathering, storing or processing the information? The significance of ownership, if the data subject is not the owner, his claim to privacy is weaker.

4. Identity theft

The digital environment and the Internet make it relatively easy to impersonate someone else, including the retrieval of additional information, unauthorized action, altering information etc.

431 See chapter 2 above (means of surveillance).

5. Distortion of information
Information given to another party that uses it without authorization and outside its context. The privacy changes according to the definition of the relationship (names, the context). Information is conceived as relevant to the relationship. It use would not be seen as a violation of privacy. The logical conclusion is that changing the context is in fact the violation of privacy, which is dependent upon the "contextual integrity" of the owner.433

6. Creating an Activity Profile
Information gathered in the course of one's activities creates a full profile, the existence of which is in itself a violation of privacy. Gathering small pieces of information can expose a person to a great extent, against his will. The profile makes it easier to manipulate the data subject.

7. Permanence of Digital Information
Digital storage means are not vanish and therefore any information gathered may be stored forever. Human memory and physical memory are vulnerable and are not permanent. In addition to the longest average life span it can be assumed that surfing the "life" of the information it will be distributed to many other destinations, as it can be copied easily. As a result of these two elements, the chances of survival of digital information are higher. The problem of this seemingly positive feature is that when incorrect, distorted or illegal information is stored without consent, its permanence may be harmful. The ability to copy and store in fact block the ability to change the incorrect information effectively. It should be stressed that when the incorrect information violates privacy, there is no public interest in such violation, which could apply in the context of correct information.434

8. The problem of concentration of information
The power to create extremely large databases containing information on an

434 CC (Jerusalem) Tal Check v. Database Registrar, 1996(2) P.M. 212,218.
extremely large number of people makes it possible to concentrate power and control, which may lead a society being controlled by database owners.

9. Loss of control over the information
This is in fact the main problem relating to databases which is also true in the context of all the other problems described above in this chapter and in theoretical chapter on privacy. This problem represents the detachment between the data subject and the database owners after the information is given or transferred.

10. Summary - The Problem of Enforcement
Having raised the problems inherent to databases, we ought to discuss the problem of enforcement. These days every personal computer is in fact a database. The hard disc can contain large, dynamic databases, raising the problems described above. If in the past the fear related to parties of power and wealth, today the distinction is blurred. The common home storage and transfer capabilities have significantly improved in the digital environment. As a result, the concentration of power in the hands of an individual is similar to that which the legislators in various countries referred to in the past as the threat to be restrained to the extent possible. Yet despite this trend, there remain gaps, especially in the ability to provide access. For example, the home computer can store an enormous sensitive and confidential database, yet granting access to a large number of people to the same database through the Internet requires further means that at least today are not commonly owned by individuals, the trends of extending bandwidths and the constant improvement of storage capabilities will narrow down these gaps, so in our opinion the legislator will eventually have to consider a completely equal power in terms of the threat to privacy between individuals and commercial companies. An attempt to regulate this issue will lead to a significant enforcement failure, as was the case with other attempts to enforce old fashioned laws in the digital age, For example, copyright of music and video files.

In this chapter we summarized the general aspects of the issue of databases, identified the place of the database in the information chain, described the database from a technological perspective and discussed in length the various problems and dangers it raises. Having laid down the foundations, we shall turn to reviewing the current legal situation with regard to databases.
C. The Current Legal Situation - An Analysis of Dangers and Objectives

Following is a review of the current legal situation in Israel, the US and the European Union with regard to privacy and data subject. In this review we combine the analysis of fears, dangers and objectives that the legislators considered.

C.1. Israel

The main law regulating databases in Israel is the PPA. After analyzing this Act, we discuss further laws, including the Credit History Service Act,\(^{435}\) and the Prohibition on Money Laundering Act.\(^{436}\) Chapter B of the PPA, dealing with databases, adopts the direct public regulation approach. We open the discussion with a short and concise historical review of legislative regulation of databases, which teach us about the legislative treatment of databases in Israel. We then describe the legislative model and the regulation of databases and finally add and analyze our comments.

1. Regulation of Privacy in Israel - A Historical Review of Databases

The Cohen Committee of 1973 dealt for the first time with the regulation of privacy. The committee lacked knowledge on computers and computerized databases,\(^{437}\) and left it for future treatment due to its complexity.\(^{438}\) The Glass Committee of 1975 understood that a speedy solution should be found for databases,\(^{439}\) as it found that there were approximately 1100 computers in Israel at the time (excluding military systems), which required handling the possible violation of privacy. The main fear was leak of information, distortion of information and profiling.

The Bill of the PPA was born when thought was given to the changing technological environment, enabling gathering and manipulation of information. Consequently the bill of 1980 provided as follows (emphasis added):

"The expansion of mass media, the development and growth of technological devices enabling monitoring, surveillance and spying,

\(^{435}\) Credit History Service Act of 2002.


\(^{437}\) According to Judge Gabriel Kling, lecture at the Neve Ilan Conference.


\(^{439}\) See the report of the committee for prevention of damage to citizens due to information stored on computers, 1981, at 6.
the growth of the gathering of information by private and public bodies and the rapid growth of the population - all of these lead to more serious violations of privacy. The individual finds himself exposed and feels that his personal intimate matters may become, without justification, public information. This new situation created the need to establish the protection on one's right to privacy and fill the lacuna on a subject of growing importance.\textsuperscript{440}

In 1986 the Public Council for the Protection of Privacy was established. It is a voluntary organization that advises the Minister of Justice on this subject. The importance of the Council is in assisting in handling the complexity of enforcing the PPA. As explained above, the enforcement failure is particularly relevant to the issue of databases. Many of the amendments to the Act are the result of the work of the Council. The Commission serves as a consultant to the Minister of Justice and the Database Registrar, and its members are lawyers, representatives of public authorities, people with technological background and others.

2. The regulation of databases under the PPA
Chapter B of the PPA - Section 7 defines a database as "a collection of data kept by an optical or magnetic device and intended for computer processing", except a collection for personal use or containing only contact details. In addition, the owner of the collection or a corporation under his control must not own further collections. It should be noted that when we use the term "database" in this part of the paper we refer to this definition.

The Database Registrar
The PPA protects the individual from gathering and processing personal information through imposing a duty of registration of databases in Israel (chapter B of the Law). A database must be registered if:\textsuperscript{441} (1) the number of data subjects therein exceeds 10,000 (2) or if it contains sensitive information, defined as "data on one's personality, intimate matters, his health, opinions and beliefs" (3) or if it contains information in people that was given without their consent (4) or if it a database a public body (5) or

\textsuperscript{440} See Bill Proposals 1453, 1980, at 206.
\textsuperscript{441} Section 8 (c)(1)-(5).
if it used for direct marketing.

The registrar responsible for registering databases has the authority to refuse the registration of a database if he or she has a reasonable ground for assuming that the database is used or may be used for illegal activities or as a disguise for such activities, or that the information it contains was received, collected or gathered against the provisions of this Law or any law.442 If the registrar makes use of this authority, the database will not be registered. Furthermore, the registrar may approve a registration application with special condition for the management of the database and its operation. If it is not registered, its operation is contrary to the provisions of section 8(a) of the PPA and is a civil tort and a criminal offence strict liability under section 31A-31B respectively. It should be noted that the registration in itself does not grant immunity against torts and offences under section 2 of the PPA that may result from the existence and operation of the database.443 Section 2(10) should be mentioned in this context, as it prohibits publishing or giving information obtained by a violation of privacy.

Section 10(c) of the PPA authorizes the registrar to supervise the implementation of the provisions of the Act and its regulations, and it appears that this refers only to the provisions of Chapter B. On March 24, 2004 the Minister of Justice set the Administrative Offences Regulations (Administrative Fine - Privacy Protection), 2004. The objective of these Regulations is to authorize the database registrar to impose administrative fines on individuals and corporations,444 amounting to hundreds of NIS and the collector is determined in accordance with the type and nature of the offence. The higher fine is imposed in cases of running or maintaining or using a database contrary to the provisions of section 8. It should be noted that the objective of these Regulations is to increase the enforcement of the database registrar. As already noted, both the supervising authorities and the registrar for many years lacked the means for enforcement. To complete the picture, it should be mentioned that before the enactment of the Act an enforcement unit had been established for the supervision, registration and securing information in databases, in accordance with the

442 Section 10(a)(1).
443 See the registrar's affidavit in CC (Tel Aviv) 1694/97 MKM General Information v. Database Registrar, Tak. Dis. 97(4), 591.(hereinafter: MKM case)
444 Regulation 2(2) - the fine imposed on a corporation if five timed the fine imposed on an individual.
needs of supervision.445

Rights and Duties in Databases
The data subject has the right to review the information gathered under section 13. The procedures were set forth in the Regulations.446 Section 14 provides that that the data subject may ask the database owner to change or amend the information about him. The database owner may refuse to this request and the data subject had a right of appeal to the court.447

The data collector, who asks for information in order to add it to a database, must inform the data subject in detail whether giving the information is obligatory or requires consent. Moreover, the collector must indicate the purpose for which the information is gathered, to whom it may be given and for what purpose.448 The purpose should also be stated when the database is registered under section 9(b)(2). The Act prohibits any use of the database for a different purpose under section 8(b). Furthermore, the database operator must maintain its secrecy under section 16. Section 17 provides that the database owner or whoever holds the information bears the responsibility for securing the information, with no details about the nature of this responsibility. Section 3(b) of the Regulations sets duties of regulating access and ongoing management of the database, keeping the information intact and reasonable security measures.449

Analysis of the provisions and their implementation
The provisions of the PPA reflect a recognition of the problems described earlier.450 Firstly, the Act deals with general dangers from which the right to privacy derives in section 2. The provisions of this section join the specific provisions in Chapter B dealing with the duties involved in running a database. It should be noted that section 2(1) of the Act and the prohibition on disusing illegal activities indicate that any legal

445 Section 10(d).
446 Privacy Protection Regulations (Viewing Information and Procedures of Appeals) 1981.
447 Section 15 of the Act and Regulation 8.
448 Section 11.
449 Privacy Protection Regulations (Holding Information and Transferring Information among Public Authorities) 1986.
450 See part 3.
fault in the information chair, which includes gathering information, storing it and using it - means that this link in the chain is invalid and so are the rest of the links that follow it.\textsuperscript{451} Of course a retroactive invalidation of earlier stages is impossible, due to the illegality of later stages. In other words, if the gathering of the information was conducted illegally, for example, if it was gathered without consent, storing the information in a database is illegal too. Any use of such information, for instance in order to send e-mail, is illegal as well, even if the use in itself is legal. It should be noted that the use of the information is illegal under section 2(10) of the PPA, even if the database was not the type that requires registration.

We now describe how the PPA treats the dangers discussed so far in this paper. The danger of leaks of information is treated by the duties of confidentiality and responsibility for security. The duties are based on the provisions of section 2 and with regard to databases - chapter B and the Regulations. The danger of distorting information are treated under section 2 and chapter B - the duty to inform the data subject of the purpose for which the database operates and the prohibition to deviate from this purpose.

The question of ownership and the division of rights is solved by section 14 - who holds a database is granted a quasi legal trust of the information. From a proprietary perspective, it appears that he has the full right to the information, including personal information. This right involved duties as described above. The right is subject to review by the courts, upon the application of the data subject. The data subject himself does not have absolute rights, but is dependent upon the review of the courts. He may browse the information, request corrections to be entered in it in order to keep it intact and may ask for it to be deleted (section 14(a)). These possibilities may enable him to try to keep as much control as possible, but it is hard to see the right to browse the information and the right to request correction as a solution for the detachment between the data subject and the information about him and to his loss of control over the information. In other words, the right of the data subject is minimal and limited.

The problem of the permanence of the information in the database is not solved by the Act. The duties regarding secrecy and security are intended to reduce the danger of a leak and distribution on the web. Furthermore, the data subject may

\textsuperscript{451} On the information chain see sub chapter 1 above.
request amendments and deletions when the information is incorrect. Yet when the
time limit for keeping the information is concerned, the Act does not include any
specific provisions. Such time limits are at the discretion of the Registrar.

The danger of profiling the data subject is tackled by the definitions and criteria
for registration, and o is the danger of concentration of information. Holding sensitive
information or information on many data subjects requires registration of the
database. The reasons and the problems involves a re described below, after we
present two important arrangements regarding databases and transfer of information
in Israel: the Credit History Data Service Act (hereinafter: the Credit History Act) and
the Prohibition on Money Laundering Act (hereinafter: PMLA). The objectives of
these two Acts are different. An essential difference between them concerns the body
holding the database regulated by them: the Credit History Act regulates the
registration of privately owned databases and PMLA regulates the registration of
databases owned by the state.

3. The Credit History Service Act
The Credit History Service Act of 2002, first proposed in 1997, provides that in
order to remove failures of economic reliability in the market and to improve payment
of debts, assist with true evaluations of credit risks and increase the competition in the
credit field for private and business clients. The main market failure identified was
the lack of information and the intent was to create a reality in which there is open
and accessible information on people's fulfillment of financial undertakings. Before
the Act was proposed, there had been several companies in the market that collected
and sold information on individuals and corporation, for example, about bad
checks. "Credit History" is the definition given by section 1 of the Credit History

453 Tana Shpanitz, "The Credit Service Law - The Final Straight" 45 Hapraklit (2005), 375 (Hebrew).
454 Ibid, at 379. The lack of information on reliability was described in a study by George Akerlof, as
causing a "negative choice", for example by creditors. If we use Akerlof's theory to analyze the credit
market where there is a lack of information, we can say that borrowers who tend not to pay their debts
are usually the clients of small creditors that do not have the resources to obtain information on their
history. The large banks that do have such resources serve borrowers who tend to pay their debts. In
this situation, all creditors in the market have an incentive to charge higher fees, and thus "good"
clients are harmed due to the conduct of "bad" clients. See George Akerlof, "The Market for "Lemons":
455 CA 439/88 Database Registrar v Moshe Ventura, 48(3) P.D. 808. As well as supra note 443.
Act to data on credit granted and refused in the past, termed "positive data" and data on non-payment of debts.

The Act was enacted in 2002 and its wording indicates that lessons were learnt from the 20 year experience of the PPA. The PPA was sometimes exploited by various bodies who wanted to hide economic information. A person who wished to hide economic information on their business could run them as an individual rather than as a corporation. His business information thus becomes economic information on an individual, protected by the PPA. This caused a problem of reliability in the market, since information on solvency could not be disclosed. Another significant problem was created in the credit market. Therefore the Credit History Act provides in section 33 that meeting certain requirements and being granted a special license allows the gathering of information on many databases running businesses as individuals, called 'traders'.

The Credit History Act is similar in many ways to the PPA. Most of the provisions dealing with rights and duties are similar in both laws. The PPA is a more general law, dealing with all types of databases. Since the Credit History Act focuses on a specific field, it is more detailed in some aspects and sometimes broader than the PPA. The two laws are not interchangeable. Section 5(a)(1) of the Credit History Act provides that registration with the Database Registrar under the PPA is one of the requirement in order to be registered as a credit data service. The Credit History Act is in fact an exception to the PPA and therefore is subject to constitutional review and is also subject to Basic Law: Human Dignity and Liberty. Therefore the Credit History Act must meet the requirement of having proportionate provisions if it infringes upon a constitutional right established in section 7 of the Basic Law. It seems that this is the reason why it contains many detailed arrangements, in order to meet the requirements of the constitutional review.

There are many rules governing the management of credit data services, the importance of which lies in the fact the law refers to more problems and dangers related to databases. Section 15 of the Act provides that an operator of a credit data service under the Law shall not engage in any other occupation, except by permission of the Registrar. This provision is intended to prevent improper management of a database due to conflict of interests. This prohibition does not apply to operators of

---

456 Sphanitz, at 377.
databases of traders only. The licensees hold significant powers. Section 24 obliges different bodies listed in the act, including official bodies, to provide data on a person to a licensee upon the licensee's request. This obligation is limited by certain quantities and qualitative condition, yet the Act anticipates those who provide information to the database from liability for offences and torts of privacy violation.

Several provisions of the Credit History Act regulate the management and storing of information, which is significantly more restrictive than that of the PPA. Section 20 provides a maximal time limit of seven years for keeping data in the database and imposes a duty to delete the data thereafter. Section 22 provides that certain types of official information are subject to even shorter time limits, after which the information cannot be sold as part of the service. Section 23 imposes a duty to indicate the time when the information was received whenever it is transferred. There is a free right to browse the information under section 30 and under section 25 the data subject can also request a report on the information included in the data subject that pertains to him. The right to amend the information is effective and significant under section 31. Any request for an amendment obliges the licensee to address the source from which the information was received. If there is no basis for the information in dispute, the licensee must delete it. In any case he must note that the information is in dispute. These provisions directly relate to the problems described in this paper - the permanence of digital information, the danger of distortion and loss of control over the information.

The Credit History Act also operates by a registration model and grants the registrar of credit services broad powers, including the power to fine a licensee, in its discretion, after we review the PMLA, we shall discuss the registration system and the problems of enforcement.

4. Prohibition on Money Laundering Act (PMLA)
PMLA was enacted in 2000, as part of a legislative move worldwide in order to combat the global funding of crime and terrorism. This move was taken as a result of the development of the ability to transfer money between countries and the growth of the protection of clients' privacy and the secrecy of the information by financial institutions such as banks. PMLA provides that private institutions providing financial services must report to the governmental money laundering authority on the activities of their clients. This duty is imposed in accordance with various criteria and giving
information is exempted from liability under any law (section 24). It should be stressed that PMLA has a significant influence on the relationship of the data subject with the database owner with regard to protection of privacy.

The main objective of this arrangement is to make it easier for the state to monitor unlawful funding and tackle a legal situation of privacy protection and secrecy. The means is the use of privately owned databases. The arrangement obliges the owners of privately owned databases not to protect the privacy of their data subjects under certain conditions laid down by PMLA, the privacy of the data subject is violated if he transfers large sums of money through a bank and the information on his activities is given to the state. It should be noted that normally the owner of the privately owned databases is not obliged to disclose the name of the data subject.

An interesting issue raised by PMLA is the potential for regulation of database management. Section 28 provides that the Money Laundering Authority is in charge of a governmental database of reports received under the Law. The Authority receives the information, stores it in the database and transfers it to various bodies under PMLA. Detailed regulations contain specific provision regarding information security. The structure of the database is described clearly and the section gives precise instructions on how the various computer systems should be divided in accordance with their functions. Information security should match a standard of security, both Israeli and international.  

5. The Problem of Enforcement and the System of Registrars

It may be that the registration duty was realistic in the past when the PPA was enacted. When there were only a few computer databases. However, in view of the growing problems in the digital age it is doubtful whether the Law fulfills its original objective. The benefit to the individual from the existence of the register is small. Beyond the registrar's authority not to register an unlawful database, we consider that the registration in itself is meaningless.

458 This is an Israeli standard number 7799, the information security standards of the Israeli Standards Institute, operating under the Standards Law 1953 the standards was adopted in the Electronic Signature Law 2001 the requirement was set in the Electronic Signature Regulations (Registration of Approval and Management) 2001. This is a detailed standard laying down many rules for security of computer systems. It is based on a British standard (BS 7799) also adopted as an international ISO 17700 standard. See also: http://www.sii.org.il/siisite.nsf/Pages/si7799.
An individual has no way of knowing in which databases he or she are included, as the information in the registry only concerns the identity of the database owner, its purposes and the types of information in contains. The registrar has no access to the databases themselves, of course.

Every individual has the right to browse the information about him in the database but obviously in order to do that he needs to know that information about him was gathered and where. This right is restricted by the Regulations, as the data subject has to apply in writing to the database owner and pay a fee in order to browse the database and the database owner may reject this application, therefore the accessibility is limited. We consider that there is room for adapting the Regulations to current changes, as today the cost of browsing the information is minimal. Perhaps encouraging people to browse the information may lead to transparency and openness, as today the applications tend to be rejected. In case of a database under the Credit History Act there is a more effective right to view the information, and perhaps some of the provisions of this Law should be adopted in the general regulation of databases. Nevertheless, only few people are aware of their right to view the information in the databases. The PPA Bill recently published by the Ministry of Justice suggests a duty on a body wishing to gather information, to add to its address a notice on the action that the data subject may take, including viewing the information and correcting it.

The Privacy Protection Registrar, in its 2002 report stated that there is a serious problem of enforcement. The Commission considers that the absence of enforcement initiatives affects the quality of life Israeli citizens and determines that in the age of penetrated the citizen is exposed to harmful, embarrassing and criminal activities.

Moreover, the Information Security Unit has suffered for many years from a serious lack of trained personnel. It would be impossible to adapt the size of the unit to the enormous resources that are required in order to supervise databases under the law. During the year 2000 the Database Register attempted to enforce registration,
following the establishment of the Supervising Unit.\textsuperscript{463} Supervisors were recruited in order to perform the tasks under section 10(e)(1) of the Act, mainly the enforcement of the requirement to register databases. Section 3 of the 2002 report by the Privacy Protection Registrar states that this registration since the year 2000 did not contribute to the protection of privacy.

Despite all the above it should be noted that some supervision does take place\textsuperscript{464} and that the registrar's office uses its power to set conditions, which makes the supervisions more proportionate and informed, and probably more effective. The actual effectiveness of the supervision and the registration system should be the subject of a separate in depth study the findings regarding enforcement cannot be ignored, and it seems that external barriers have been in the way of the supervisors, such as budgetary barriers. Nevertheless, we are under the impression that the registration system itself is a substantial barrier on the way to effective protection of privacy.

On the other hand, the latest moves should be viewed in a positive light, namely the Administrative Offences Regulations (Administrative Fines - Privacy Protection), authorizing the registrar to fine violators and granting her with an effective, imminent and practical tool to realize the objectives of the Act. The bill of the amendment to the Act suggests that the responsible minister be authorized to exempt certain databases of the registration duty due to their size, the type of information or their purposes, and this is likely to make the enforcement more effective.

The Israeli legislator was one of the pioneers in regulating the registration system, with time, as the system was implemented in various European countries during the 1980s it seemed as the appropriate method of enforcement.\textsuperscript{465} We should not the as discussed in section 4c belowm the new general model in Europe does not includes registration system. It is still used in dome countries in Europe but we predict that they will align themselves with the general model of European legislation, creating a central supervising authority with broad powers for the protection of privacy. The Privacy Protection Commission recommends the adoption of the European model for several reasons: firstly, because the euro legislation is most

\textsuperscript{463} Privacy Protection Order (Supervisory Unit) 1999.

\textsuperscript{464} According to the database registrar, Adv. Yossefa Tapiero at the Neve Ilan Conference.

\textsuperscript{465} According to Adv. Haim Klugman, chairman of the Public Council for the Protection of Privacy, Neve Ilan Conference.
progressive; secondly, because the legal situation in Israel makes it harder for it to join European treaties and agreements related to information transfer between Israel and EU countries. This affects the private market on both sides.

C.2 The European Union

1. The EU - between free market economy and privacy protection

A central principle in the EU is a vision of market economy based on the free movement of capital, commodities, people and services. As a commodity, information transfer should be free, yet the need to protect "personal" information has been recognized in Europe. This is the manifestation of privacy in a world of new free economy, which is supposed to provide freedom of almost all restrictions.

The value of privacy is protected under section 8 of the European convention on Human Rights (ECHR)\textsuperscript{467} section 8(1) provides that" Everyone has the right to respect for his private and family life" and the violation of privacy may be permitted under four conditions, according to section 8(2) and the relevant case law:\textsuperscript{468} 1. In accordance with the law; and 2. The law is clear enough, so the data subject can plan ahead; 3. The violation is necessary 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, or for the protection of the rights and freedoms of others; and 4. The violation is "necessary in a democratic society" and is proportionate to the purpose it serves.

The constitutional duties under section 8 apply to public authorities yet some of them can apply to private bodies too. Firstly, a certain state can pass legislation that applies section 8(1) to the private sector. Furthermore the case law holds that the duties of private bodies should be balanced against the public interest and that of individuals. This balance includes the purposes defined in section 8(2). To sum up, it appears the European Court may approve the application of rules to protect personal


\textsuperscript{467} Convention for the Protection of Human Rights and Fundamental Freedoms.

\textsuperscript{468} Kamiel J. Koelman, "Privacy, Data Protection and Copyright: Their Interaction in the Context of Electronic Copyright Management System, \url{http://www.ivir.nl/publications/koelman/privreportdef.pdf}. 
information in the private sectors well.\textsuperscript{469}

2. The Regulation of Databases in the European Union
In the field of keeping information and privacy information there are two directives, forming sets of principles accepted by the institutions of the EU and should be adopted by the member states through national legislation.

\textbf{Directive on the Protection of data - 1995}\textsuperscript{470}
This Directive regulates the subject of data protection, with the aim of removing the obstacles for free movement of information, without surrendering the protection of personal data. As with any European directive, the fundamental purpose is to harmonize the legislation and policy of all EU members. This Directive deals with data privacy, rules on data processing, databases and so on. However, the issue of privacy on the web is not specifically referred to. The question can be raised of how the directive can be applied to the internet, but we must remember that it is technology neutral, in the sense that it is supposed to supply an answer to a legal problem when raised in the context of different technologies. Processing of personal data is broadly defined and almost any action in relation to the data is seen as processing.\textsuperscript{471} The data subject is entitled to be fully informed of any processing of data about him, as far as possible and subject to the law. He also has a right of access to the data, including inquiries on whether the data appear in the database, which data appear and what is the source. He may receive a copy of the data and amend any incorrect datum. He has a right to learn about the guidelines of automatic systems processing the data, and he may discuss the rationale behind their operation and to oppose any determinations made on the basis of incorrect data.

The directive sets criteria for transfer and processing of data, as follows: fair and lawful processing,\textsuperscript{472} gathering data only for a specific, express and legitimate purpose and us in accordance with these principles,\textsuperscript{473} the data should be appropriate,

\textsuperscript{469} Ibid, at 37.
\textsuperscript{470} Directive 95/46/EC on the Protection of individuals with regard to the processing of personal data and on the free movement of such data.
\textsuperscript{471} Ibid, article 2(b).
\textsuperscript{472} Ibid, article 6(1)(a).
\textsuperscript{473} Ibid, article 6(1)(b).
relevant and not excessive in relation to the purpose for which it was gathered,\textsuperscript{474} the data should be kept up to date.\textsuperscript{475} Those who control the data must give the data subject reasonable means to amend, delete or block incorrect data about him.\textsuperscript{476} In addition date used to identify a person should not be kept for a longer period of time than necessary.\textsuperscript{477} Section 7 requires that data be gathered only with full consent of the data subject and when needed in order to perform a contract or under law.

The above principles formulate the manner in which data are gathered by private bodies, another restriction is derived from the duty imposed on public authorities in Europe not to give data to private bodies, except where necessary in the public interest or where the private body shows that the data is required and the interests of the database will not be harmed as a result.\textsuperscript{478}

The directive also imposes a duty on every member to establish a supervising authority or a commission to implement the directive,\textsuperscript{479} with a duty to report to it on data processing.\textsuperscript{480} It should have powers of investigation, prosecution and receive complaints from citizens.\textsuperscript{481}

Another substantial provision in the directive in this Directive imposes a duty on member states to ensure that when data pertaining to European citizens leaves the borders of the EU it is appropriately protected.\textsuperscript{482} This provision is particularly important because it has an educational effect on countries outside the EU, for example. When a European organization is interested in trading with an American organization, it may be expected that the European level of privacy shall prevail.

To sum up, it should be noted that the Directives, like almost all parts of European law, are subject to significant exceptions. In European law there is recognition of the importance of the conflict between the right to privacy and other

\textsuperscript{474} Ibid, article 6(1)(c).
\textsuperscript{475} Ibid, article 6(1)(d).
\textsuperscript{476} Ibid, ibid.
\textsuperscript{477} Ibid, article 6(1)(e).
\textsuperscript{478} Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data http://europa.eu.int/comm/internal_market/privacy/docs/application/286_en.pdf.
\textsuperscript{479} Ibid, article 28(1).
\textsuperscript{480} Directive 95/46/EC article 18(1).
\textsuperscript{481} Ibid, articles 28(3) and 28(4).
\textsuperscript{482} Ibid, article 25(1).
freedoms and interests, such as the freedom of speech and security. Therefore there are exceptions that allow violation of privacy and data protection when certain justifications exist. The justifications include mainly law enforcement, detection of crime and protecting other persons' rights. In fact, any member state can include different exception in its local law out of the list provided.

The Implementation of the 1995 Directive
If we take the UK as an example, privacy protection in that country is very weak.\(^{483}\) Enforcement and public awareness of this issue are increasing but are still very low and far from satisfying the privacy guaranteed in section 8 of the ECHR. The European regulation system of principles set in directives, failed and one of the reasons for this is that site owners that gather information do not know clearly what the law requires of them and the enforcement is not substantial\(^{484}\)

Nevertheless, there are positive signs of future implementation of the Directive. The Data Protection Act of 1998 enacted in the UK and implementing the provisions of the 1995 Directive, is enforced by the Information Commissioner that reports that most private business which process personal data do report on this as the Act requires of them.\(^{485}\) The duties imposed on an individual or a company holding personal data on other, not for their persona use only (in case of an individual) are clarified on the Information Commissioner's website, so every citizen has a simple way to find his duties\(^{486}\) and the it is also possible to file a complaint through the website.\(^{487}\)


\(^{484}\) Ibid.


\(^{486}\) http://www.informationcommissioner.gov.uk/.

\(^{487}\) The user can print out the complaint forms and they are simple to fill out, so every citizen can use them (http://www.informationcommissioner.gov.uk/eventual.aspx?id=32.)
The 2002 Directive

The directive concerns the processing of information in electronic communication services. In relation to databases, the main provisions are that wherever electronic or printed data exists every person may be excluded from the list without cost. In order to secure the information transferred through public electronic network, section 4 of the directive imposes a duty on suppliers to take steps to guarantee a secure service to their clients, when the demand is not complete security, but a level a security appropriate for the nature of the information. When there is a risk of the data being exposed, the service provider must inform the users of this risk and of potential remedies for the legal problem.

Confidentiality of the data: Section 5 provides that receipt of tapping of data without the users' consent is prohibited. There is further restriction to his provision in matters of security (see above). The directive also provides that traffic data should be saved only for the purpose of defense against claim for inaccurate billing. Use of the data for commercial purposes can only be made with the user's consent. With regard to databases containing data on clients it provides that the clients have the right to determined whether their personal data should appear on public lists of the company and opting out of such lists should be free.

The Implementation of the 2002 Directive

The member states that adopted the principles of the 2002 Directive into their national laws before the deadline (October 31, 2003) were Denmark, Spain, Italy, Austria and Sweden. In the UK, regulations went into force adopting the directive on December 11, 2003 and they contain detailed provisions on users' rights in the cellular market, telephony and e-mail, as required in the directive.

This directive was approved in 2002 by the institutions of the EU and went into force. As a result of its short life span there is currently little experience regarding its implementation. It is evident that a significant part of its principles and certainly the


489 Ibid, article 6.

490 Ibid, article 12.

guideline have become an integral part of the national laws of the member states. The question of their implementation in practice remains open at this stage, especially in view of the partial success of the 1995 directive regulating the processing and gathering of data without referring to a specific areas.

C.3. The United States
1. Privacy Legislation in the U.S.
Under U.S. law there is no general protection of privacy, yet there are specific prohibitions in certain fields, such as such as types of technology, types of information gathered or types of bodies and institutions. The American perception sees privacy protection against the state as significant and justifying direct regulation. However, privacy protection against private commercial bodies is less important as the regulation of the private market should be achieved by the market forces.

The use of the American constituting that does not provide a clear defense to a person against privacy violations by private bodies cannot grant full protection. The American constitution provides protection from the state only on certain matters. Professor Solove shows how the combination of this partial protection and the wrong interpretation given to privacy over the years led the courts to problematic and even wrong conclusions.492 The way privacy is treated s influenced by the "big Brother" paradigm and interpreted as the right to secrecy and protection against invasion into the private domain. Solove shows how the courts created a rule under which personal data which is already known to third parties and private bodies and is no longer secret - cannot be considered as protected by the right[. Even where the constitutional protection is clear, as against the state giving information, information open to the public will reach private hands in any case and can be included in commercial databases.

Solove draws analogy between the U.S. PPAs and patches.493 He argues that they may protect various activities that violate privacy, but not the main activities the information on which is open to the public. The American legislation is clearly market oriented, unlike the European legislation, and in a sense Israeli legislation too. Any information open to the public, the process of which is not prohibited in a specific

492 Solove, at 1430-1445.
493 Solove, at 1444.
law, is used freely by the market of private databases for profit while violating privacy. Another problem is that the data subject usually has no idea that his privacy is violated. Constitutional protection is better than tort but is still lacking.

Following are several examples of laws on information security, gathering information authorizing access to information and data processing.

**USA PATRIOT Act**

Although the American perception gives greater weight to the threat of the state, this Act, enacted following the September 11 attacks, contradicts this perception. This is a controversial Act that grants ISPs immunity from claims by user where the ISP gives information by the request of the state. The FBI can force any body to give information or records on its clients. The government can browse financial records, health files, reading habits, surfing habits etc. some of the provisions of this Act expire on 2005, but the authorities are preparing a permanent substitute, the Domestic Security Enhancement Act.

This Act has a great influence on the issue of ISPs' databases, as it allows the authorities forced access and retrieval of data from databases, processing and cross processing it with data from other sources. This Act raises the fears described above regarding privacy violations, such as leaks of information, distortion and the problem of ownership. The Act realizes the danger we have discusses, when information in a private database owned by a service provider is given to the state as already noted, this Act annihilates the public law protection the limits the activities of the state.

**Intelligence Authorization Act for Fiscal Year 2004**

This Act grants the FBI wide authorities to obtain reports of financial institutions without a warrant. As a result, there is no need to show any cause in order to obtain information. Under the USA PATRIOT Act the FBI could only obtain information with a warrant by a Federal judge and other intelligence agencies could obtain financial data with the approval of a senior government officer. However, section 374 of the 2004 Act presents a relatively lenient requirement, under which the FBI agent


must declare that the data gathered is fundamental for a security investigation. Another significant change is the definition of a financial institution that is broader under this Act and includes insurance companies, travel agencies, real estate agents and even the postal service.

The new Act prohibits the business owner being investigated with regard to specific data or a specific client from telling that client that he is under surveillance. This is of particular significance, as it forces the database owner to act in a manner which is contradictory to the theoretical principles discussed above. This Act appears to be the most "total" law among the laws that allow privacy violations in the U.S. Unlike the US PATRIOT Act, granting immunity to database owners, this Act turns privacy violations secret, hidden from the data subject. The extension of the definition of financial institutions infringes upon the reasonable expectation of privacy protection while there are institutions in which the violation of privacy is closer to the data subject's expectation, the Act is intended to treat other institutions in the same manner regardless of that principle. U.S. legislation also deals with the activities of private commercial bodies, for example:

Privacy Regulation by the FTC

The Federal Trade Committee enforces a provision which existed before the Internet era, prohibiting misrepresentation. Where a body that gathers information declares that it has a certain privacy policy and breaches its commitments, the FTC can impose serious sanctions. A privacy policy is a type of private regulation laying down a series of rules, that may include, for example, rules on leaks of information, the permanence of the information, information distortion, profiling and in fact all the problems mentioned above. This provision is important for two reasons. Firstly, because the FTC has effective power, and secondly, because this is an indirect version of basket protection of privacy, considering the clear difference from direct regulation. This is an example of indirect public regulation in which the prohibition is not explicit and does not pertain to a specific matter, but prevents violation of privacy as it may have a chilling effect on electronic trade, the information trade being an important part thereof.

Gramm-Leach-Bliley Act\textsuperscript{497}
This Act provides that any financial institution must protect the secrecy and the security of personally identifiable information of its clients. It also provides that clients should be informed of the bank's privacy policy and have access to information gathered and the ability to correct it. The Act prohibits pretexting, namely stealing financial information through impersonation. It clearly expresses the fear of the dangers of identity theft, information leaks and other dangers.

The Cable Communication Policy Act (CCPA) - Section 551\textsuperscript{498}
Under this Act there is a duty to inform a subscriber of personally identifiable information when entering into an agreement for cable service or other communications services. The subscriber must be given a written notice of (a) the type of information gathered on him and the ways in which it is used; and (v) the nature, frequency and purpose of any disclosure of information including the type of person to which it is disclosed; (c) the period of time for which the provider keeps the information; and (d) the access to information

The service provider must not gather information or give it to others without the express consent of the subscriber, and he must secure the information, allow the subscriber convenient access to it and the opportunity to correct it. The provider must destroy the information he does not require for his purposes (defined as the nature of use of the information).

2. Analysis of U.S. Legislation
Despite the tendency to suspect the government, the terrorist attacks in the past few years led to a fundamental change in the American perception of privacy and the ability of the give to gather and save information previously seen as private. The result is a change in terms of the definition of the threat, so it appears that privacy protection against the state has surrendered to security needs. Examples can be found in the USA PATRIOT Act and the Intelligence Authorization Act, in addition it is evident that as the special legislation regarding private bodies is expanding, these also present a threat to privacy in the American industry the traditionally governing

\textsuperscript{497} 15 U.S.C. §6801 et seq.
\textsuperscript{498} 47 U.S.C. §551.
approach of that of fear of congress intervention in the market through direct public regulation, therefore there is demands for preventative private regulation by a declared privacy policy. The problem is that privacy policies normally do not prevent the manipulative use of information.

Secondly, the wish to protect personally identifiable information in particular is evident, as opposed protecting any type of information. This distinction becomes vague due to the development in the American information area.

Governmental plans intended to provide technological tools for gathering and monitoring information, at the beginning of the century operated together with the development of technologies for privacy protection during the gathering of information. Lately it was reported that the funding for the privacy protection plans has been stopped so in practice, the plans for gathering information still exist while the plans for protection have been abolished.

Another conclusion we can draw out of the legislation on private bodies is the importance given to informing a person about the fact that information about him is gathered and uses of it. The requirements of service providers emphasize the need to show these beyond any doubt, except in cases of security needs. Such provisions indicate the wish to allow a person to control the information about him or the flow of information about him. It can also be seen that the U.S. law does not tend to be technologically neutral, does not avoid using technical and technological terminology in the legislation, due to the conception of regulating specific areas.

D. Solutions
Following are several essential issues in finding solutions to the problem of databases:
1. There is a need for special legislation with regard to computer databases with regard to protection of privacy;
2. There is a need to increase awareness and education about responsible conduct in society in general, about the risks involved in using the web and particularly about

---

499 One of these bodies is DARPA which operated until recently (http://www.darpa.mil/body/pdf/FINAL2003FactFileref1.pdf); another body is ARDA, which currently coordinated the development of means for gathering information (http://www.ic-arda.org/about arda.htm). On the DARPA plan see Simson Garfinkel, Database Nation (Beijing, O'Reilly, 2000), 249-250.

500 The plans that have been abolished are Genisys and Bio-Alert: http://customwire.ap.org/dynamic/stories/T/TEEROR_PRIVACY?SITE=COCOL&SECTION=BUSINESS.
disclosing information;

3. The European and Israeli approach, supporting direct public regulation of privacy in general and the issue of databases in particular, is essentially correct. A central privacy protection institution is called for, preferably a public non-governmental authority, and in any case, an independent authority;

4. It is doubtful whether the existing arrangement under the Protection of Privacy Act, whereby a duty of registration is imposed, can still stand;

5. The powers of the supervising institution should be wide enough in order to enable effective and active enforcement. The powers should include imposing specific conditions and limitations on certain types of databases, on databases in a particular area of occupation or field of industry, limitations on specific database owners and on specific databases. The supervisor should have the power to impose administrative sanctions, such as fines, closing down businesses and imposing personal liability on managers (subject to a just procedure and the rules of administrative law, of course). The supervising body should be allowed, for the purpose of supervision, to inspect and examine the databases and to receive complete information on their management. The option of allowing the supervising institution full access to the databases should be considered, where there are reasonable suspicion and other guarantees, in order to prevent abuse of power;

6. Submission of a complaint to the supervising body should be as free as possible, without fees. The Internet should be used as a low cost, efficient tool for serving the citizens;

7. The data subjects should be allowed access and to the data on the databases, and this should be as free as possible, considering the sensitivity of the information. Clients should be informed of the information about them being accumulated and of their rights with regard to such information, in a complete, convenient and low cost manner. For example, when the information is already on the Internet for the use of company employees, it should also be disclosed to the relevant clients. Where databases are disclosed on the Internet, substantial weight should be given to the interests and rights of the database owners and their business conduct.

8. In addition, private regulation and self regulation of privacy protection in running databases should be encouraged. It should be enforced in a similar way to the US FTC, namely through indirect public regulation, that encourages private regulation. The use of the law of tort can be effective in regulating privacy protection. Incentives
should be created in order to encourage self regulation, its maintenance and self enforcement;

9. A body holding public information should be recognized as a quasi-public body. Such a body is subject to duties and norms of conduct and management derived from administrative law, or at least the parts of administrative law imposed on quasi public bodies under Israeli law. Examples include the duty of transparency, the Freedom of Information Act, the duty to give reasons for and exercise of discretion in a reasonable and proportionate way by the database operator, all of which combined will create a greater degree of fairness in the database environment.

10. A private body not holding public information, but holding a large amount of information or particularly sensitive information - we ought to consider imposing similar duties when the information it holds is essentially similar to public information.

11. Any regulation of computer databases depends on stable, comprehensive and well-defined legislation in the general field of computer crime.
4. Privacy at the Workplace

A. Introduction

The industrial revolution and technological changes have created a state of affairs in which a person is identified with his or her occupation, measured according to it and spends most of his or her life in self-realization through work. It is difficult to divide one's personal life and his "working hours", especially in the fields of economy and technology, as the word has become a commercial global village.

The right to privacy is in conflict with economic interests. On the one hand, protection of privacy increases the social cake, as a person is considered more productive when free from external intervention. On the other hand, protection of privacy involves investment of resources and has a high cost. In the area of labor law the conflict is greater, since apart from the public interests, the proprietary right of the employer should also be considered. The employer wishes to maximize his profits and have full control of the means of production, and these may include the employees' working time and their use of resources. The employer is also interested in protecting trade secrets and avoiding vicarious liability for the employees' acts. Yet if we take the view that it is hard to distinguish between our working life and our leisure time, protection of the employees' privacy gains greater significance.

Studies in the U.S. show that employees "waste" about 25% of their working day on using e-mail and surfing the Internet, and that one of every five companies has fired an employee due to inappropriate use of e-mail. As a result, the expenses of information security and system administration grow, the employees' productivity decreases, and the employer has an immediate need to supervise the surfing and the use of e-mail by the employees. On the other hand, the negative effects of following employees should be taken into consideration. According to management theories, a non autonomous employer is less efficient and less creative. Studies shoe that surveillance is detrimental to efficiency, morale and trust among employees.

---

502 Dalia Zelikovitiz, "Surfing the Internet at the Workplace" [http://www.nfc.co.il/articlesprintversion.asp?docid=1497&subjectid=3](http://www.nfc.co.il/articlesprintversion.asp?docid=1497&subjectid=3) [Hebrew] "Assuming an organization employs 1000 employees and each of them spends 'only' two hours a day surfing and sending emails (out of 8 hours - a quarter of the working day), these are 2000 working hours a day or, if an employs works 260 days a year - 520,000 lost working hours."
Whereas in the past the means violating privacy, such as sudden visits, cameras and phone tapping required substantial resources for the violation of privacy and for analyzing the findings and drawing conclusions, today the information age offers technological tools that make control, monitoring and processing of information by the employer easier, while also making it easy for the employee to expose information.

This chapter discusses the problems raised in employment relationships in the information age, in the context of privacy in the digital work environment. First, we shall present the technological tools that enable violation of privacy of employees, with short technical explanations and examples. Then we shall examine the consideration that should be taken into account in formulating a solution, from the point of view of the employer, the employee and the public interests. In the search for a solution we shall present the approaches adopted in the U.S., in Europe and the legal situation in Israel. We shall conclude with a suggested solution, referring to the possible form of regulation, the desirable regulation and the problems involved in its implementation.

B. The Technological Means for Violation of Employees' Privacy

These days there are several means for following employees' action, some of them are as of as employment relationships are, such as attendance cards, sudden visits etc. Some of them are in use since the beginning of technological developments in the end of the 20th century, such as cameras and phone tapping. Here we focus on the technology developed in the 21st century to follow the employee in the digital environment. Before reviewing there, we shall remind ourselves of some general terms:

| Computer Address: An ID number for a computer on a network, depending on the type of network and the communications protocol used to transfer data. |
| Communications Protocol allows for communications between computers by |

---

504 We do not address other privacy concerns in the employment relationship, such as tests for candidates or surveillance in the physical environment.

505 For example: 1) on an internal network, this is normally a Mac Address, an address belonging to a physical communication device; 2) IP Address, containing 32 characters, linked to a single station.
attaching a "Header" to each message sent on the network. It usually includes the address of the destination computer, the source computer and the integrity of the information.\textsuperscript{506}

**Local server**: A computer on which a program is installed enabling the administration of the list of end-computers (computer addresses), their authorizations (usually in accordance with the username) and their requests for information. The local server administers the resources and regulates the contents of the information transferred according to definitions.

**Ethernet**: A network based on a communications protocol enabling unique identification of every computer in the organization, using the local server.

**Router**: An electronic device with several ports matching the number of computers connected, and one port. The port is normally connected to the server the router has a table used to find routes for the various computers.

**Ethernet Connected to the Internet**: the computers in the organization not used as servers do not have direct access to the Internet. They gain such access by sending a request to the local server, directed by the router to the appropriate server.

**Port**: A single physical port divided into logical ports. The definition usually refers to a logical number through which the information is transferred.\textsuperscript{507}

### B.1. Monitoring E-mail

Many workplaces provide the employee with an e-mail address. It should be noted that this is not merely a virtual address, but it requires allocation of disc memory for storage of the messages. Therefore, the employer, as owner of the service, apparently is allowed to do as he wishes. Some employers run a program that searches for certain

\textsuperscript{506} The information depends on the type of protocol, for example, the basic communication model is based on the seven layer model, and the application is in use (the browser, e-mail software etc) ignored the need to add details such as information verification. Such data is added automatically. Andrew S. Tanenbaum, *Computer Networks* (4 ed. Prentice Hall, 2002)
key words in e-mail messages, and some go further and examine all incoming and outgoing messages on a selective basis (when they have an interest in following a particular employee).

**Technical Explanation**

An outgoing e-mail message sent through an organizational computer is transferred to the router and then to the server for storage. Later on, according to the allocation of resources by the server, the message is sent to its destination on the Internet. Among other things, an e-mail message sent within the organization goes through the same process, apart from the final stage (the gateway to the Internet). The internal message goes back to the router to be transferred to the destination computer within the organization.

It is important to note in this context that all messages are saved on the server and usually also after their transfer, for backup. An e-mail surveillance program is installed on the server and identifies a request from the organizational computer is that of sending an email, it ignores the destination address and the message goes through the usual stages (integrity check and rendering it readable by e-mail software). Therefore the program can examine the attachments, search for key words in the contents and subject line etc. It should be noted that these actions can be performed in relation to specific senders and recipients, as this information is included in the message before it is rendered readable by e-mail software.

**B.2. Monitoring Surfing**

Access to the Internet in many workplaces is considered essential. However sometimes it is impossible to restrict access only to specific sites. The employer is interested to know that his employees are investing their time in work only, therefore he maintains a log of the sites the employee visits and the time spent on each site. This is later analyzed, and often the employee is reprimanded and only then does he realize that he was followed.

**Technical Explanation**

Each request for information is logged by the server and contains the information on the source computer, the information requested and the time. Deleting one's history files from one's own computer does not change the functioning of the surveillance
program, as it searched the logs on the server. The program can search the requests, and each of them can be processes, using the same technologies used for filtering contents, namely searching for keywords in the site contents, the name of the site and meta tags. It calculates the time spent on the site and the time spent surfing in general, usually by calculating the differences between the requests of information from the Internet, ignoring statistical amoralities due to leaving the browser open or automatic requests.

B.3. Filtering Contents

Often the employer wished to prevent the distribution of certain information, such as trade secrets or access to sites such as pornographic sites, and therefore uses programs for blocking and filtering sites and e-mail messages, defined by keywords. Although this is not pure violation of privacy, under a wide interpretation this infringes the employee's freedom and may amount to violation of privacy. Therefore it appears that we need to discuss this in view of the many options the employer has of controlling transfer of information.

Technical Explanation

Filtering programs operate when the request is sent from the Internet, there are three main technologies in this area:

1. Blocking the port, according to the types of software the employer wishes to block.

2. Creating a close list of sites that employees are permitted to visit for the purpose of their work. Each request is matched with the list, and if the site requested is not on the list, the employee will be denied access.

3. Filtering sites with certain words appearing in their names, contents or meta tags. Normal the blocking is done in accordance with the name of the site or its meta tags, as any other option may compromise the system performance.

Nevertheless, it should be noted that filtering programs are not perfect. They may block too many sites or fail to block certain sites.

---

508 A meta-tag is a short description of the site, usually used by search engines.
509 See chapter 1 above.
510 Kazaa, for example, uses a certain port, therefore an employer wishing to prevent its use should block that port.
B.4. Monitoring Software Installed

Normally, in order to fight viruses and avoid copyright breaches, the employer scans the employee's computer in order to find harmful software or software without license. Outside the working hours, a program scans the computer registry and the hard drive. The list is usually given to the employee with a notice on deletion of the software found, yet sometimes the employer may delete them without the knowledge or consent of the employee.

**Technical Explanation**

A program performs a scan of the registry and the map file.

*Registry*: a file containing the list of programs installed on a workstation, their licenses and other relevant information about where they are installed.

*Map file*: a file containing information in physical addresses of the programs installed, requests for resources by the programs and the use made of the.

The scanning program is run by the main program installed on the main server and it usually operates outside working hours. It should also be noted that although the program runs an agent on the computer, it cannot be discovered by untrained user who does not have a system administrator authorization. The program ignores licensed software and reports on unlicensed software or software with privately bought licenses.

B.5. Examples of Surveillance Programs

Following are several examples of programs that demonstrate the technological means described above:

**E-Blaster**

The program sends a periodical e-mail report about any activities on the employee's computer. It records and reports to the employer about all software used, all websites visited, all chat session, the time each activity lasted and anything typed, including a screen shot at the time of the report. It can be set to send a report whenever a certain word is typed. It operates in the background without the user's knowledge.

A PRO Agent\textsuperscript{512}

The program captures screen shots and displays them as video movies; it remembers anything typed in any Windows program, including passwords, e-mail, etc. It identifies and saves transcripts of chats on MSN, AOL, Yahoo! and ICQ.

Spector Pro\textsuperscript{513}

The program saves e-mail messages (incoming and outgoing) according to set criteria. This program also follows web-based e-mail accounts such as Hotmail and Yahoo. It follows the employee's surf and typing.

Cyber Patrol\textsuperscript{514}

This is a program that blocks access to a set list of web sites, it filters sites according to keywords.

C. Considerations in Formulating a Solution

Having reviewed the background, we shall now turn to examine the guiding considerations in formulating a solution, and then review the legal situation in several countries and suggest our solution.

C.1. The Employee

Right to Privacy: surfing, email and installing software indicate the employee's personality. In view of the fact the most of our lives is spent at work, we are vulnerable at the workplace to various interaction, proceeding on the assumption that privacy is a value worthy of protection, the privacy of workers at the workplace should be protected. The violation of privacy is even more substantial in the case of surfing surveillance, contents filtering or surveillance of software installed. Surfing surveillance can violate one's privacy when a deduction is made based on the sites he visits and his persona details,\textsuperscript{515} especially when such information is taken out of

\textsuperscript{512} http://www.spyshop.co.il/index2.asp

\textsuperscript{513} www.spectorsoft.com/products/SpectorPro_Windows/

\textsuperscript{514} http://www.cyberpatrol.com.

\textsuperscript{515} For example, if a person visits homosexual sites this may indicate his sexual tendency, or if he visits medical sites it may indicate health problems, and so on.
Freedom of Speech: the employee's freedom of speech is infringed both directly and indirectly. Indirectly - because the violation of privacy creates a "chilling effect" deterring the employee from expressing himself. For example, an employee who wished to expose irregularities at the workplace while preserving his anonymity may avoid it for fear that he may be found out. The freedom of speech is directly infringed, if we assume that free surfing is protected under the freedom of speech. The assumption is that surfing is a means of communication, a source for acquiring information and knowledge and an area in which one can express himself. Thus surfing realizes the freedom of speech and the employee should be protected from the employer's arbitrary censorship. The greatest infringement is filtering contents, but as we can see from the examples described above, it is possible to prevent sending emails containing certain keywords, and this creates an infringement as severe as site filtering, as the employer can almost completely prevent discussions of some subjects at the workplace. Yet, it seems that the direct violation is not as strong, in view of the fact that the employee can communicate with his friends and surf without limitation outside working hours, beyond the reach of his employer.

The employee's expectations: often the employee expects that her privacy will not be violates when she surfs the Internet and sends e-mails. It should be noted that expectation is influenced by the employee's culture and the work environment in general and with a certain employer in particular. The workplace environment is a product of the extent of the Internet access at the workplace, but also of informing the employees of the means taken, and a real possibility of gaining their consent. On this subject there is no uniform opinion regarding all the possible violations of the employee's privacy and the level of expectation is created according to the various violations and the information given to employees. Therefore we should consider a situation in which the employer argues that the employees have been informed of the possibility of surfing surveillance, from which they should have concluded that e-mail surveillance can also be performed. In this case, it appears that the employees were given insufficient information.

C.2. The Employer

The employer's property. The resources at the workplace belong to the employer, as does the employee's time. Obviously, the employee himself does not belong to the employer. Therefore it appears that the employee has the right to act in order to protect his property. In addition, he has to protect his intellectual property: trade secrets, copyright and patents. This central issue has implications with regard to the extent of the violation of privacy, as appropriate filtering and surveillance according to certain keywords and/or descriptions relating to the employer's property (trade secrets), rather than general.517

The employer's duties. The employer is subject to many laws imposing liability on him in case of negligence by employees and determining his vicarious liability.518 Therefore the employer can be expected to comply with the legal standards and defend himself against potential claims. For example the Jerusalem Magistrates' Court found SuperPharm liable to pay damages for libel on the company's internal e-mail network.519 Another cause for liability is the Prevention of Sexual Harassment Act.520 The employer may be liable for allowing, even in an implied manner, for the creation of a sexually hostile environment.

The employer's needs. Often the employer acts in order to prevent virus attacks on the computer system, break ins into the computer, exposure of trade secrets and so on. We should note that the employer can achieve this by means that violate privacy to a lesser extent, such as anti virus programs.

C.3. The Public

Employment relationships: Granting legitimacy to the theory of labor law which is appropriate from the social perspective is a public interest that ought to be protected (the appropriate doctrinal framework being, for example, public policy): this is a transformation from the perception of the employee as an "object" owned by the

517 For example an employer who make surveillance programs ought to use the keyword "surveillance", rather than monitor e-mail in general.
518 For example for not preventing sexual harassment, breach of copyright, defamation and torts.
519 CF (Jerusalem) 1269/02 Meir Azulai v SuperPharm, Tak. Supr. 2003(1), 54.
520 Section 7 of the Prevention of Sexual Harassment Act 1998.
employer to one the views the employment relationship as based on equality, with the need to protect one group in order to prevent exploitation. This consideration leads to protection of the employee's privacy. The problematic issue is whether privacy should be granted cogent protection of permitted to be waived, and in which circumstances.

The working environment: changes in the working environment make the said difficulties even greater. Industry today is moving from production to services. In the hi-technology industry, for example, the employment relationship is not limited to time and space (due to copyright considerations and the link to the global economy). Therefore the employee may often work from home, using the equipment and resources of the employer, and there is no clear line between working hours and leisure time. This reality entails the reexamination of the rights and duties of employees and employers. The use of certain technological means at the workplace can be appropriate in some contexts but their use on the personal computer at the employee's home may excessively violate his privacy and that of his family members.

*Economic efficiency* and preventing waste of resources are also public interests that ought to be protected. Therefore to the extent surveillance at the workplace is intended to prevent a decrease in productivity, it should not be forbidden (although it may be that rules should be set in relation thereto, as discussed below).

Technology. A legal policy must take into consideration the technological implication it creates. The arrangement should be neutral in term of the, as the change in technology are frequent and the adaptation of legislation is often too late. We should not restrict the extent of the desirable arrangement to the technological means in use at the moment, since it will become irrelevant tomorrow. Son the other hand, we ought to consider the fact that any arrangement that forbids the use of a specific technology for surveillance will hinder the development of technology in future.

*Third party rights*. When the employer monitors outgoing e-mail messages, these usually contain information on third parties to which the message is sent, or from whom it is received. In the balance of consideration third party rights infringed as a result of such monitoring should be taken into account.

**D. Existing Public Regulation**

In this sub chapter we shall review the existing law in the U.S., Europe and Israel, in each jurisdiction we shall examine the historical background leading to the current law, as we as the legal principles the legislations and examples from the case law.
D.1. The United States

The history of labor law in the U.S. reveals hostility by the legislator and the courts towards trade unions and workers' rights.\textsuperscript{521} It is interesting that in a nation once divided over the subject of slavery, employees' rights are of lower significance than employers' interests. Other issues related to labor law, such as the definition of employment relationship, there is an evident change of approach in the case law and a move from the "master and servant" approach to defining an employee in accordance with the purpose of social legislation.\textsuperscript{522} However, with regard to workers' rights, a conservative attitude is preserved, whereby the employee waives some of his rights at the workplace, or does waives his rights to some extent.\textsuperscript{523} Historically this position can perhaps be understood if we accept the assumption that the American Civil War and the struggles against slavery were incidental and that the reasons for that war were mostly unrelated to slavery.\textsuperscript{524} The trends in the U.S. are more suitable to a capitalist society, which is apparently a more important value that certain human rights, or, as Milton Friedman put it, it capitalism that guarantees freedom a different trend can be seen in Europe, despite the fact that the main dispute regarding slavery is not in Europe, but as we shall seem it may be that the fear of social exploitation and returning to the feudal period in history led the Europeans to adopt this approach.

The Fourth Amendment to the U.S. Constitution establishes the right to privacy in the context of searches and seizures, as against the state.\textsuperscript{525} The Constitution does not apply in the private sphere, but common law tests have been formulated, regulating the issue in the private sphere. The two main tests developed under U.S. law to cover the right to privacy at the workplace, including the expectation test and the contents test.\textsuperscript{526} The former focuses on the employee's reasonable expectation of privacy at the workplace (an implementation of the general expectation test under

\textsuperscript{521} Tony Adams, "Employers, Labor, and the State in Industrial Relations History: A Reply to Gospel" 51 The Econ. History Rev. 597 (1998).

\textsuperscript{522} US v. Silk, 331 US 704 (1947).

\textsuperscript{523} Frederick S. Lane, The Naked Employee (2003).

\textsuperscript{524} Arnon Gottfeld, From Colonies to a Civil War - American history until 1861 (Tel Aviv, 1986) (Hebrew).

\textsuperscript{525} "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated..." Amend. IV.

\textsuperscript{526} Eli Helm, Privacy Protection Act (2003), 433 (Hebrew).
U.S. law, based on the *Katz* case, and the latter examines the contents of the information and the extent to which the employee's privacy has been invaded. The first test is an objective one and called "a circumstantial approach", examining the reasonable expectation according to the work environment.\(^{527}\) The employee's expectation of privacy has been examined mainly by the employer's declared and implied privacy policy.\(^{528}\) The case law has recognized some of the employer's interests that grant legitimacy to violations of privacy, for example, avoiding legal liability due to sexual harassment by e-mail.\(^{529}\) At the same time, there exists an approach that supports the narrow interpretation of this exception, whereby the extent of the violation compared to the protected interest.\(^{530}\) This approach is linked to the second test, the contents test, which imposes a duty on the employer to prove a "business interest" and a reasonable level of invasion of privacy.\(^{531}\) The U.S. courts have substantially narrowed the employee's right to privacy on computer systems and in most cases ruled that he does not have an expectation of privacy on computer systems.\(^{532}\) It should be noted that this is a two-part test, making it harder to prove the violation of privacy, since only after the employee proves that he had a reasonable expectation of privacy, the invasion and its justifications are examined, namely the level of expectation is not proportionate to the extent of violation, and it may be that the employee fails to prove reasonable expectation, and a substantial violation can escape the test.\(^{533}\) U.S. case law draws a distinction between the state as an employer and private employers. It was held that the Fourth Amendment prohibiting searches without warrant applies to the state not only as a law enforcement authority, but also as an employer.\(^{534}\) We discuss private employers.

The Electronic Communication Privacy Act of 1986 (ECPA)\(^{535}\) applies to employment relationships with regard to monitoring employees' e-mail messages by

---


\(^{528}\) *James v. Newspaper Corp.*, 591 F.2d 579, 581 (10th Cir. 1979).


\(^{530}\) *Sanders v. Robert Bosch Corp.*, 38 F.3d 736 (4th Cir. 1994).

\(^{531}\) *Watkins v. L. M. Berry & Co.*, 704 F.2d 577 (11th Cir. 1983).


the employer. An employee can agree to such monitoring, and there are also exceptions that enable the employer to monitor emails, for instance when the employee knows of it in advance and it is needed for maintenance or for protection of the employer's property. Under the courts' interpretation of this Act, its provisions refer to monitoring e-mail messages only while being sent, and not when stored on the server. Lately the court repeated this ruling and held that the Act does not apply to monitoring messages stored temporarily on a computer, but only while they are being sent. Since this is only a very short period of time and technologically the employer can read the messages stored on the server, the Act is in fact been made an empty shell. This approach is compatible with the liability imposed on employers with regard to offensive e-mail (harassment, discrimination) and of publications by their employees. In addition, there is an academic approach whereby the employee does not have an expectation of privacy at the workplace, as the system administrator has access to the e-mail messages of all employees.

Following the September 11 terror attacks, ECPA was amended by the USA PATRIOT Act. Stored e-mail messages are now covered by the Act, but the court ruled that an employer is considered a communication service provider under the Act, and is therefore exempt from liability. ECPA grants protection to communication service providers and exempts them in cases of surveillance by virtue of their role the court once more made the aw into an empty shell by ruling, by defining each employer as a communication service provider under the Act. It should be noted that the court acted in accordance with the rationale of that protection, by allowing the employer to perform maintenance and protection activities, but the result is that the employer is free to perform other acts that violates privacy with no justification.

In the past few years the there has been a growing trend of firing employees due to inappropriate publications and use of e-mail. Consequently, public discourse on the

536 It was held that an employee who signs a document allowing the employer to conduct a search has no reasonable expectation of privacy. American Postal Workers Union v. United States Postal Service, 871 F.2d 55 (1989).
537 Steve Jackson Games, Inc. v. U.S Secret Service, 36 F.3d 457 (5th Cir. 1994).
538 United States v. Councilman, 373 F.3d 197 (1st Cir. 2004).
constitutionality of monitoring e-mail messages has grown. The courts support the employers' rights and have ruled in *Smyth v. The Pillsbury Co*[^542] that despite the employer's promises about not monitoring e-mail in order to base dismissals, there is no right to privacy of e-mail on the company's network.

**D.2. Europe**

Privacy and freedom of speech are protected under section 8 and 10 of the European Convention on Human Rights (ECHR) respectively. Violation of these rights is permitted only in order to protect the rights of the state or other individuals. Establishing those rights is traditionally linked to the vertical balance (between the state and the individual), but in terms of the horizontal balance (between individuals) there is not explicit determination about the application of these rights, although it is clearly necessary.

In the 19th century an employee was viewed as a servant.[^543] One explanation for this perception is the social situation where the ownership of the means of production was analogical to ownership of knowledge and technical abilities.[^544] In the past, countries with a legal system based on a civil code (continental Europe), relinquishing workers' rights was conceived as something derived from the subordination of the worker to his employer, while in common law countries, relinquishing such rights was not seen as a necessary result of the employment relationship defined by the control test, based mainly on control of time and division of work.[^545] The labor law in Europe developed in the direction of the common law and although the tests changed following the technological revolution that divided management from knowledge at the workplace, thus creating the integration tests and economic reality for the definition of employment relationships, the perception of workers' rights is still evident in granting more power to the employee in the organization. The explanation if apparently the socialist views common in Europe and learning the lessons of the past.

The European approach attempts to balance between the employer's need to

[^542]: Pillsbury, supra note 532.

[^543]: *Yemens v. Noaks* (1880) 6 QB 530.


follow the employee's work and the employee's right to privacy. As a general rule it has been held that the employee does not relinquish his privacy once he enters the workplace. Among other things, it is suggested to examine whether monitoring is necessary and transparent and whether the results cannot be reached by other means that violate privacy to a lesser extent.\textsuperscript{546} The focus in the European approach is on prevention and education. The employer should provide guidance and direct the employees' conduct as he wishes, rather than relying on discovering forbidden conduct and imposing sanctions. Therefore the employer is under duty to inform the employee of surveillance.

The European Court of Human Rights held that the employee's privacy should be included in the right to privacy, as for most people a significant part of the day is dedicated to work and most of their relationships with the outside world are established at work.\textsuperscript{547} In a ruling on phone tapping, the court stressed the need to inform the employee as a basis for his expectation - as long as the employee has no reasonable base for believing that he is being monitored, he is presumed to expect privacy. The Court held that use of technological means falls under the protection of privacy, and the question that remains open relates to the conflict between the right to privacy and the employer's rights. The location and the ownership of technological means do not affect the extent of the right to privacy.\textsuperscript{548}

Following are several examples of the implementation of the abovementioned section 8 and 10 by European states:

1. **Germany**: Protection of privacy in the media is established in the German constitution. In addition, section 85 of the Telecommunication Law requires every telecommunication service provider to keep the information transferred in the network confidential. Monitoring business e-mail is permitted only with prior consent of the employees without which there is no right to supervise the efficiency of their work. In any case, monitoring and reading private emails is not permitted, even with consent. Therefore it is recommended to use two e-mail addresses: private and public. The same rules apply to monitoring surfing, under the Protection of Information in

\textsuperscript{546} Article 29 – Data Protection Working Party, 5401/01/EN/Final/WP 55 (29 May 2002).
\textsuperscript{547} Niemitz v. Germany (1992) EHRR 97.
\textsuperscript{548} Halford v. United Kingdom [1997] IIHRL 59.
Communications Services Law.\textsuperscript{549} However, computer systems may be monitored in order to protect them against viruses.

2. **UK**: The RIPA\textsuperscript{550} provides that an employer is not allowed to monitor employees' phone conversations and e-mail messages without explicit consent by the sender and the recipient. The employer had broad defenses under the Telecommunications Act\textsuperscript{551} allowing him to monitor employees' activities without their consent in the following cases preventing crime; connection to an organization/workplace; preventing imminent system failure, investigating and detecting system break-ins and demonstrating the standards which are achieved by the employees. These defenses are broad but the employer must information the employee of the possibility that his use of the system may be monitored according to those exceptions.

3. **Belgium**: Section 22 of the Belgian Constitution established the right to privacy. In addition, a collective agreement imposes a duty on the employer who wishes to use new technologies at the workplace, which may affect the working environment, such as for surveillance and gathering information, to provide the employees' representative with information on these technologies and their natures and to explain why they are needed and how they will operate.\textsuperscript{552} Moreover, the confidentiality of correspondence is protected under section 109 of the Reform of Certain Economic Public Companies,\textsuperscript{553} preventing tapping of any kind of information between people through media without consent. The Belgian Information Security Organization issued a document about monitoring employees' e-mail and surfing,\textsuperscript{554} under which and employer is not entitles to monitor e-mail, as this is not proportionate to any legitimate interest the employer may wish to protect. Instead, the employer should monitor their employees' emails according to criteria of quantity and traffic or use special programs to detect exceptionally large messages or chain letters. With regard

\begin{itemize}
\item \textsuperscript{549} Utilization of Teleservices Act § 5 (TDG).
\item \textsuperscript{550} Regulation of Investigatory Power Act 2000 (RIPA).
\item \textsuperscript{551} Telecommunication (Lawful Business Practice) (Interception of Communication) Regulations 2000.
\item \textsuperscript{552} Article 2, s.1 of the Collective Agreement nr. 13 of 13 December 1983.
\item \textsuperscript{553} Article 109 d, The Reform of Certain Economic Public Companies, 21 March 1991.
\item \textsuperscript{554} The Belgian Data Protection Authority, Opinion no. 10/200 of 3 April 2000.
\end{itemize}
to surveillance of surfing it was held that permanent surveillance is inappropriate. Therefore the employer must prepare a general list of sites, without identifying the employees who visited them, and then evaluate the extent of the harm cause, and if it is substantial, the employee should be asked for explanations.

4. Finland - On 1 October 2001 the Protection of Privacy in Working Life Act\textsuperscript{555} was enacted in Finland, in addition to the existing Privacy of Information Act. The Act applies to both the public and the private sectors, and includes work applicants. Section 9 of the Act refers expressly to employee surveillance. The objective of the Act is not to create a system of rights and duties inked to the technological means or to the use of existing information networks, but to encourage the formulation of policies at the workplace. The act stresses that the employer should not prejudice the privacy of the employee private emails. Any information gathered by means of surveillance must be a necessary part of the employment relationship. The Act also imposes a duty on employers to consult employees before implementing policies regarding monitoring emails. After consulting the employees, the employer must define the purpose of the surveillance and methods to be used and policies for using e-mail and databases.

D.3. Israel

The right to privacy is protected by Basic Law: Human Dignity and Liberty and the PPA. The relevant causes of action for violating privacy by employers are included in the PPA in section 2(1) (spying), 2(2) monitoring, 2(5) (copying), 2(7), 2(8) confidentiality and 2(9) (personal affairs). In addition, the employer has duties with regard to maintaining a database, and especially informing the employee about gathering information and for what purpose.

It appears that section 2(5) of the PPA is the most appropriate one. Spying (section 2(1)) requires proving harassment; monitoring under section 2(2) is forbidden under the Secret Monitoring Act (discussed below); breach of confidentiality under sections 2(7) and 2(8) applies only in situations where this duty exists; and use of information on one's personal affairs and section 2(9) is relevant where conclusions are drawn from the information gathered through monitoring the surf, rather than

\textsuperscript{555} Protection of Privacy in Working life Act, 1/10/2001 Finland.
emails. Under section 2(5) copying the contents of a letter or other written documents without permission is forbidden. In order to use this section in favor of the employee, we should prove that e-mail can be defined as a letter or written document, in order to adapt the law to the technological changes, as opposed to the views that see section 2(5) referring to paper documents only, contrary to the spirit of the Act.\textsuperscript{557} In addition, the issue of the employee's consent should be examined in this context, as the section refers to the employee's permission and it is also required by section 1 of the Act.

The PPA protects the employer from liability for privacy violation in circumstance where there is a legal duty to commit such violations (section 18(2)(b)), a need to protect a legitimate interest of the employer (section 18(2)(c) or violation committed in the course of lawful business activities (section 18(2)(d)). However, these defenses are subject to the employer's duty not to violate the employee's privacy to an excessive extent, also derived from his duty to act in good faith under section 18(2). In addition, the extent of the violation of privacy and the employer's interest should be balanced, under section 8 of Basic Law: Human Dignity and Liberty, requiring proportionate means in violation of basic rights.

The protection of the right to privacy at the workplace is also covered by the Secret Monitoring Act.\textsuperscript{558} Section 1 thereof provides that a "conversation" includes "computer communications"; "secret monitoring" is defined as "monitoring without the consent of any of the participants in the conversation". In order to implement the defenses granted under this Act, two main problems should be solved: the first refers to the employee's consent, since if the employee consents to monitoring his e-mail, there is no "secret monitoring", as one of the participants consented. The issues raised in this context are of the type of consent (express or implied) and the extent to which the employee is informed.

The second problem refers to the definition of "conversation" in the technological context of computer communications. In the Netvision case it was held that the police may read e-mail messages unless they are monitored while being

\begin{footnotesize}
\leavevmode
\begin{itemize}
\item \textsuperscript{556} Supra note 438 at 440.
\item \textsuperscript{557} Supra note 2 at 113.
\item \textsuperscript{558} Secret Monitoring Act of 1979.
\item \textsuperscript{559} Supra note 438 at 439.
\end{itemize}
\end{footnotesize}
sent. It is clear that this is only a short period of time. However, in the case of Badir it was held that listening to voice mail messages is considered "monitoring" for the purpose of this Act.

Basic Law: Human Dignity and Liberty forbids in section 7(b) entering into one's property without premising and section 7(c) prohibits search in private domain, and section 7(d) prohibits the violation of privacy of correspondence. The National Labor Court held in a series of cases that the provisions of the Basic Law apply to the private labor law, whether directly or indirectly, and the employee's right to privacy at the workplace was stressed in the Zim case; the National Labor Court heard a claim regarding the interpretation of collective agreements and the imposition of basic rights norms, at the base of the Israeli legal system: "the provisions the law should be interpreted in a manner compatible with the basic principles of the system in general, while granting an appropriate balance to each principle freedom, right and so on". This case it was also held that "avoiding the retroactive abolishment of rights" and "respect for basic rights of members of the organization". In order that the provisions of the Basic Law can aid the employee, we should examine whether the private domain includes e-mail messages and sites surfed at work. If we accept the approach that the employee has a quasi-proprietary interest in his workplace, then it may be that the personal computer, including the e-mail box, can be viewed as "private domain" for the propose of the Basic Law, and any limitation, surveillance or filtering constitute entering the public domain of the employee.

With regard to the type of consent, it was held in the Tel Aviv University case on the legality of tests for potential employees, that waiving the right to privacy can be viewed as contrary to public policy and is therefore void. The wish to be accepted to a workplace and to be promoted leads the employee to waive his right to privacy and to consent to many acts that violate his rights at work. The National Labor Court,

560 MC 090868/00 Netvision Ltd. v IDF, (Not yet published).
561 Dialogues such as chats can be distinguished from monologs such as e-mail correspondence. The former can be seen as a conversation under the Law, while the latter may fall under this definition of the time between sending the e-mail and receiving the reply is short.
563 Dovrat Sharam v. Globes et al
564 Hahistadrut Haklalit v. Zim,
565 Tel Aviv University v. Hahistadrut Haklalit.
discussing the right of the University to compel employees who apply for internal tenders to undertake tests that invade their privacy and being aware of this situation, examined the employee's consent in a different manner than consent given in different circumstance, and therefore held that "an employee's decision to undertake the tests is not always given in free will."566 The absence of free will consent is considered as absence of consent, thus the violation of the employee's privacy is against the law. This rationale is also valid with regard to monitoring the employees' activities, as it invades their privacy, and their consent cannot always be considered as free will consent.567 This case uses constitutional tests derived from Basic Law: Human Dignity and Liberty with regard to the validity of violations of individual rights. It was held that it should be examined whether the violation has an appropriate purpose and is proportionate. It should be noted that the University is a public body, or at least quasi public and therefore is naturally subject to the these constitutional tests is natural.

E. Towards a Solution?

To a large extent the question of privacy at the workplace is mostly regulated privately by market forces and technology. From the standpoint that assumes a market failure in the sense that the labor marker has always had a power gap between the employee and employer, as explained below, technological protection of privacy by the employee is not effective, it appears the public regulation (direct or indirect) is needed, in addition to the existing public regulation of privacy in general. The application of the general law (the PPA and the Secret Monitoring Act) to the employment relationship is no an obvious one.

The extent to which the employee can control his or her privacy at the workplace is highly limited, even more than in other situations. In most cases the employee is not permitted to install software on his computer, which may prevent the violation of privacy and in most cases the activity that violates privacy is not conducted on the personal computer, but on the servers, to which the employee has no access. An immediate technological solution to the problem is use of private

566 Ibid.
technological tools, such as a laptop with Internet connection through a cellular phone, but such a solution is not available to most employees today. Furthermore, contractual regulation is not applicable either, as the power divide between the employee and the employer will lead to the employer's position prevailing, and since the employee would prefer social benefits to his right to privacy, which he might waive. In addition, it should be noted that the right to privacy is vague in terms of its extent, which creates a certain misunderstanding about its importance, both by the individual (the employee) who does not know his rights and is willing to waive them without realizing their significance, and by the state, entrusted with the role of enforcing such contracts, and lacks understanding of the depth of the right to privacy and its position on the scale of rights, therefore there is not effective enforcement.

The conclusion is that in order to grant effective protection of the employee's right to privacy, public regulation (direct or indirect) is needed. To determine which approach is preferred, we should examine the advantages and disadvantages of each. It is evident that the European approach tends towards protecting the employees' rights, unlike the U.S. approach, which avoids a clear decision on the issue and leaves the regulation to the market forces. It may be that the differences derive from the different economic approaches and the American capitalist system, aspiring for maximizing profits and market efficiency, while believing that the best decision will be taken in a market free from legislative intervention. However, the Europeans support governmental regulation, based on the belief that the legislator ought to balance between the interests of the employer and employee.

The general law in Israel does balance between the interests of the employer and employee, by setting defenses in the PPA, but it lacks clarity with regard to the terminology used and its applicability to the digital environment. There is also lack of clarity with regard to the employees consent, linked directly to the employee's expectation of privacy at the workplace.

Since we consider that in employment relationship we cannot trust private regulation by the market forces, the European approach, based mainly on expectation and informing the employee - is the appropriate approach. It is not dependent on technology, unlike the U.S. approach. Moreover, the expectation is examined in

---

568 For example the unclear definition of "monitoring" under the Secret Monitoring Act, as reflected in the case law.
accordance with the extent of the violation. The employee's consent should be examined in accordance with the expectation and taking into account the power divide - it seems that the informed consent approach discussed in the first chapter can be applied in this context too. The informed consent reflects the fear of coercion by the employer and the lack of full knowledge by the employee. However, informed consent can be ineffective in this context, it can always be said to be given due to some pressure. A possible solution may be found in collective agreements, discusses below.

A solution for the problem of consent can be the applications of public law tests of proper purpose, proportionate means and the absence of an effective alternative. In addition, a "routine" situation should be distinguished from an "unusual" situation (for instance, fear of confidential information being given to competitors). The employee must be informed of routine monitoring and consent to it. However, when the employer monitors the employees' activities due to suspicions of unlawful acts (or contrary to company policy) - he does not have to inform the employees in advance, but this monitoring should be reviewed in light of the tests of proportional means and absence of alternatives. Moreover, the test of proportional means should distinguish between monitoring contents and specific activity. Whereas the former can hardly ever be justified, the latter can be justified in the absence of alternatives.

The combination of indirect public regulation, in the sense of giving incentives to employers who protect privacy, through partial exemption from vicarious liability when use is made of technological tools owned by the employer (under certain criteria). For example, the Anti-Defamation Act can provide for an exemption from vicarious liability for employers who protected their employee's privacy, leading to him not preventing the defamation. Employers' will have the incentive to protect privacy preventing the dilemma of whether the employer should protect privacy and be exposed to vicarious liability to violate privacy and be vulnerable to claims. It should be noted that the same purpose can be achieved through creative interpretation of section 18 of the PPA but obviously old legislation has the advantage of certainty which is very important in the private sector.

569 The test laid down in the O'Connor case, supra note 533.
570 See Chapter 1.c above.
571 Supra note 565.
Other possibilities include setting a threshold for the protection of employees' privacy and regulating the matter under the collective labor law, because although the trade union and the collective agreements are becoming weaker, they still constitute a central factor in the labor market in Israel. This can be done by regulating the issue of privacy in collective agreements, either general and/or for a specific workplace. The use of collective agreements is also compatible with the movement from the perception of labor law as a matter of status (where the employee has little influence on determining the rules in the employment relationship) to an approach that views the employment relationship as a contractual matter. Provisions regarding privacy in a collective agreement belong to the normative level of the agreement (between the employee and the employer) and therefore raise a problem of enforcement, for two main reasons:

1. An employee may not sue due to fear and the employer may exploit this;
2. The economic damage to the employee cannot be quantified or is negligible and does not form an incentive to sue.

There are several solutions to these problems:

1. Allowing the trade union to bring action based on a normative provision, regulating the right to privacy and make it an obligatory provisions (namely, one that applies as between the employer and the union). In addition, we can consider establishing joint committees of the employer and the trade union under legislation, to discuss the disputes relating to violation of employees' privacy.

2. Class actions, allowing a number of employees to bring action together, in order to solve the problem of quantification mentioned above, and this may also decrease the fear of harm to a specific employee.

It appears that a solution based on a collective agreement balances between the employee's right to privacy, freedom of speech and expectation and the employer's property, duties and needs, since collective agreements can be adapted to different occupations and allow for flexible rules compatible with the existing reality on the labor market, while encouraging the protection of privacy due to public policy and allowing freedom for technological developments. Even if a collective agreement is not technologically neutral, it will still apply to a trade union and not form a general

572 See Dan Or-Hof's article above.
restriction on a specific technology. On the other hand, the suggested solution raises problems since it requires time and makes the regulation dependent upon the negotiations between the employers and trade unions. In order to encourage them to set rules on privacy in collective agreements, it is suggested to use indirect public regulation to give incentives or to impose a duty to include such provisions in collective agreements, while creating a mechanism for expanding the applicability of a collective agreement in accordance with the type of employer or market sector, and supporting the waive of the right to privacy only when agreed upon between the employer and the trade union, as this reduces the power divide.

F. Summary
In order to provide effective protection of the privacy of employees, public regulation (direct or indirect) is required. Direct regulation should be similar, in our opinion, to the European approach, which focuses on informing the employee. The advantages of this approach are the technological neutrality and examining the employee's expectations in accordance with the extent of the violation of his privacy. A possible solution for the problem of the employee's consent to the violation of his privacy is examining the employer's activity under the administrative law tests of proper purpose, proportionate means and the absence of an effective alternative. In addition, a "routine" situation should be distinguished from an "unusual" situation at the workplace and monitoring contents should be distinguished from monitoring activity.

Direct regulation can also be achieved by creating incentives for class actions on violation of employees' privacy.

Under collective labor law, the trade union should be able to bring action against the employer for violation of employees' privacy. In addition, we can consider establishing joint committees of the employer and the trade union under legislation, to discuss the disputes relating to violation of employees' privacy.

Combined with the direct regulation, we should also consider indirect regulation, giving incentives to employers to protect the employees' privacy (for example, partial exemption from vicarious liability when use is made of technological tools owned by the employer). Additionally, indirect regulation can be part of existing collective agreements.

573 Such as extension orders.