Cornell International Law Journal

Volume 37
Issue 1 *2004*

Article 2

The Struggle of a Democracy against Terrorism - Protection of Human Rights: The Right to Privacy versus the National Interest - the Proper Balance

Emanuel Gross

The Struggle of a Democracy Against Terrorism—Protection of Human Rights: The Right to Privacy Versus the National Interest—the Proper Balance

Emanuel Gross†

† Professor, Faculty of Law, Haifa University. Former Military Judge in the Israel Defense Forces, holding the rank of colonel. Thanks are due to my research assistant Ms. Tchia Shachar, whose dedicated work enabled this article.

37 CORNELL INT'L L.J. 27 (2004)

Introduction

> What distinguishes war conducted by a state from war conducted by its enemies—one fights in accordance with the law, and the other fights in contravention of the law. The moral strength and substantive justification for the authorities' war depend completely on compliance with the laws of the state: in waiving this strength and this justification for its war, the authorities serve the purposes of the enemy. The moral weapon is no less important than any other weapon, and perhaps even surpasses it—and there is no more effective moral weapon than the rule of law.[1]

Since its establishment, the State of Israel has been subject to incessant terrorist attacks. Streets, buses, and places of mass entertainment transformed in the blink of an eye into fields of death is not the scene of a nightmare but a daily reality. The cost of terrorism is unbearable. The lives of thousands of innocent civilians have been brutally cut short, and the existence of tens of thousands of injured men and women has been changed unrecognizably; the Israeli experience is suffused with bereavement, pain, frustration and anger. Coping with the constant fear of imminent terrorist attacks imprints its own indelible mark on every aspect of daily life, political, cultural, social and economic.

On September 11, 2001, the full force of terror struck at the heart of the United States. The sights were familiar to Israel, as was the profound sense of shock that swept over the American people. History will not record the attack of September 11th as the first hostile action taken against the American people; however, in terms of the number of victims, the extent of the destruction, the methods by which it was carried out, and the degree of defiance it exposed, it was an assault more threatening than any that had preceded it. It led the President of the United States to declare war against terrorist organizations throughout the world[2] and it inspired his allies to join him.

What measures may a democratic state properly take to protect itself in times of emergency? Clearly, not every measure is permissible. Both in times of peace and in times of crisis, it is the legal norms that set the boundaries for what is permissible and what is prohibited. Although the

1. High Court of Justice [H.C.] 320/80 Kawasma v. Minister of Defense, 35(3) P.D. 113, 132 (Heb.).

2. U.S. President George Bush's speech before Congress and the American people, delivered on September 20, 2001, *available at* www.whitehouse.gov/news/releases/2001/09/20010920-8.html (last visited Aug. 5, 2003).

law does not fall silent in times of war, it may occasionally permit a deviation from the legal norms applicable in times of peace. In its hour of crisis a state is not required to sacrifice itself on the altar of the basic rights and freedoms of its citizens but is entitled to restrict these rights and freedoms as is necessary to effectively deal with its enemies:

> There is no choice—in a democratic society seeking freedom and security but to create a balance between freedom and dignity on one hand and security on the other. Human rights cannot become an excuse for denying public and state security. A balance is needed—a sensitive and difficult balance—between the freedom and dignity of the individual and state and public security.[3]

The real, and perhaps most difficult, test of a democratic state lies in its ability to draw a proper balance between these two competing values, which will prevent the imposition of avoidable restrictions on individual liberties.

Finding this balance is not an easy task. Difficult legal questions are accompanied by a number of moral dilemmas. This Article is not concerned with finding the proper fundamental balance between the interest of national security on one hand and the entire range of individual liberties and rights on the other; rather, it is concerned with identifying the balance between national security and a human being's fundamental right to privacy.

A terrorist attack cannot be defined solely as the accomplishment of the terrorist's aspirations. A terrorist act is the completed external expression of a catalogue of preliminary activities—planning, preparatory work, financing, training, and qualification—clandestinely carried out by the terrorists while exploiting the state's lack of watchfulness over activities carried out in the realm of its citizens' private lives.

Accordingly, it is easy to understand why, after every attack, and more compellingly after an attack that produces multiple casualties, the question that echoes in every quarter is why the intelligence services failed to identify those preliminary activities: Was it because the modern surveillance measures were not sufficiently sophisticated? Was it because, despite the availability of sophisticated intelligence devices, constitutional restrictions prevented their use? Or was it perhaps that, despite the efficacy of the measures and the absence of constitutional obstacles to their implementation, the intelligence personnel were simply negligent in the performance of their duties?

History teaches us that the erosion in the public's sense of personal safety brought about by the sights of carnage and destruction, combined with feelings of pain, anger, and the desire for revenge, generally lead the public to assign the blame for the tragedy to the constitutional restrictions and therefore to conclude that those restrictions must be removed and a new balance drawn between human rights and the public interest in

3. Further Hearing [FH] 7048/97 Anon. v. Minister of Defense, 54(1) P.D. 721, 743 (Heb.).

national security. Alexander Hamilton eloquently expressed this public feeling as follows:

> Safety from external danger is the most powerful director of national conduct. Even the ardent love of liberty will, after a time, give way to its dictates. The violent destruction of life and property incident to war, the continual effort and alarm attendant on a state of continual danger, will compel nations the most attached to liberty to resort for repose and security to institutions which have a tendency to destroy their civilian and political rights. To be safer, they at length become willing to run the risk of being less free.[4]

However, history also teaches that after the security crisis has passed, it generally becomes evident that there was no rational factual basis for sacrificing rights in favor of security needs and that the lifting of the constitutional restrictions was no more than the emotional product of panic, paranoia, and fear.[5]

What, therefore, is the proper rational balance that must be drawn between protection of the privacy of the citizens of a state on one hand and the security interest in invading the public's privacy on the other, which would allow the security authorities to identify those few who would exploit the right to privacy to plan and execute acts of terror?

The trail I shall follow to identify this balance begins in Part II, which is devoted to clarifying the legal and moral importance of the two competing values: I shall look both at the difficulty in defining and clearly delineating the boundaries of these values and at their justification and significance in a democratic society. In Part III, I shall review the various ways that are available to invade the private life of an individual, beginning with traditional human detective methods and ending with a range of surveillance technologies, which are daily becoming more complex and sophisticated. In Part IV, I shall examine Israeli law on these issues and in Part V, I shall turn to a comparative analysis of the legal arrangements applied in the United States, Canada, England, and the European Union, placing special emphasis on the legal changes that followed the terrorist attack of September 2001. Part VI, which concludes this article, examines the constitutionality of the various countries' arrangements from a comparative perspective and cautions against the dangers entailed by extreme and irrational legal responses.

I. The Moral and Legal Nature of the Clash Between the Right to Privacy and National Security Interests

A. The Right to Privacy

At all times, in every society, the individual desires to maintain a certain amount of distance from the rest of society; the cultural relativism of

4. THE FEDERALIST NO. 8, at 67 (Alexander Hamilton) (1961).

5. W.J. Brennan, *The Quest to Develop a Jurisprudence of Civil Liberties in Times of Security Crises* in NATIONAL SECURITY AND FREE SPEECH (Kluwer, Sh. Shetreet, ed., 1989).

societies influencing societies' character.[6] Notwithstanding, or perhaps because privacy is such a deeply rooted value in human culture, the vast literature in this field teaches us that it is one of those concepts that everyone understands but that cannot be defined in an objective and descriptive way that clearly expresses the scope of its application.[7] In fact, over the years, numerous efforts have been made to define the term. The most important and influential definitions may generally be placed in one of three categories:[8] *first*, privacy is defined with the aid of the concept of moral rights and claims. Thus, for example, it is described as the right of the individual to be left alone,[9] as a claim to freedom to decide in what circumstances and to what extent information about the person will be divulged to others[10] and, as a corollary, the person's right to live part of his life far away from the prying eyes of the public.[11] *Second*, privacy is defined in terms of control. Among other things, it is described as the individual's control over the dissemination of information about himself,[12] his control over the quantity and quality of the information concerning himself that is made known to others,[13] his control over his body, his place of residence, his identity and information about himself,[14] and his control over the extent of the public's knowledge of his private affairs.[15] *Third*, privacy is defined in terms of accessibility. Thus, for example, it is described as that which prevents the unwanted access of the public to the individual on three levels: the level of secrecy (access of the public to information concerning the individual), the level of segregation (access of the public to the body and premises of the individual), and the level of anonymity (physical—as opposed to mental—attention of the public to the individual).[16]

The grounds for privacy are instrumental in nature and are twofold:[17] on *the individual level*, privacy plays a central, and sometimes critical, role in realizing the aspirations, desires, hopes and goals of the individual.

---

6. For an extensive anthropological review, see A. WESTIN, PRIVACY AND FREEDOM 13 (5th ed. 1968).

7. J.C. INNESS, PRIVACY, INTIMACY AND ISOLATION 3 (1992).

8. F.D. Schoeman, *Privacy: Philosophical Dimensions of the Literature in* PHILOSOPHICAL DIMENSIONS OF PRIVACY: AN ANTHOLOGY 2-4 (F.D. Schoeman ed., 1984) (hereinafter PHILOSOPHICAL DIMENSIONS).

9. Privacy is "[t]he right to be let alone," in the words of Warren and Brandeis, adopting the expression coined by Judge T. Cooley. *See* S. Warren & L. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

10. WESTIN, *supra* note 6, at 7.

11. M.C. SLOUGH, PRIVACY, FREEDOM AND RESPONSIBILITY 3 (1969).

12. A.R. MILLER, THE ASSAULT ON PRIVACY 25 (1971).

13. C. Fried, *Privacy (A Moral Analysis), in* PHILOSOPHICAL DIMENSIONS, *supra* note 8, at 210.

14. D. MCLEAN, PRIVACY AND ITS INVASION 49 (1995) (quoting Robert Ellis Smith's definition).

15. H. Gross, *Privacy and Autonomy*, in PRIVACY 169 (J.R. Pennock and J.W. Chapman eds., 1971).

16. R. Gavison, *Privacy and the Limits of Law*, 89 YALE L.J. 421, 423 (1980); S. BOK, SECRETS: ON THE ETHICS OF CONCEALMENT AND REVELATION 11 (1982).

17. C.J. BENNETT & R. GRANT, VISIONS OF PRIVACY: POLICY CHOICES FOR THE DIGITAL AGE 101-03 (1999).

First, privacy is an essential condition to formulating the individual's personality:[18] the ability of a person to comprehend the uniqueness of his existence relative to the existence of other people is dependent on his capacity to personally experience physical and psychological events and thereby conceive his separateness from the whole. *Second*, privacy is an expression of human dignity:[19] open invasion of a person's privacy compels him to plan his actions while taking into account the public that has been forced on him and that judges those actions. Clandestine invasion of his privacy changes the state of affairs on the basis of which he acts and prevents him from making considered behavioral choices in the light of existing objective circumstances. In both situations, lack of respect for the individual's desire to distance himself from others (in the absence of justifiable reasons) expresses disrespect for him. *Third*, privacy is an essential condition for the creation of interpersonal relations, in general, and deeper relations based on feelings of love, friendship, trust, and respect, in particular.[20]

Accepted social mores dictate the type and scope of participation in information that is appropriate to the different types of relations conducted by people. Without privacy, everyone has the same quantity and quality of knowledge concerning a person, with the result that he will not be able to create different relationships on different strata. Deep relationships rely on the individual exposing certain facets of his personality to the other party to the relationship. Lack of privacy prevents him from concealing these facets from the outset and thereby prevents him from creating a relationship that is separate from and deeper than those relations he normally has with the public at large.

Fourth, privacy is an essential condition for intimacy.[21] A person who participates in an intimate experience submerges himself in it, whereas an inherent aspect of an onlooker's perception is the sense of relative detachment from the event that is being observed. Awareness of the presence or the possible presence of an uncalled for spectator, compels a person to examine his acts from the perspective of the onlooker, and the detachment caused thereby prevents him from plunging into the intimate experience. *Fifth*, privacy helps an individual to concentrate, to be calm, and to refrain from criticism and ridicule[22] because, as noted, the absence of uncalled for observers frees a person from the distraction inherent in being watched; privacy will make it easier for the person to remain calm and concentrate on the range of creative human activities, by virtue of which he can enrich his spiritual world, acquire knowledge and skills, and develop his intellec-

18. J.H. Reiman, *Privacy, Intimacy and Personhood*, *in* PHILOSOPHICAL DIMENSIONS, *supra* note 8, at 310.

19. S.I. Benn, *Privacy, Freedom and Respect for Persons*, in PHILOSOPHICAL DIMENSIONS, *supra* note 8, at 223-44.

20. J. Rachels, *Why Privacy Is Important*, *in* PHILOSOPHICAL DIMENSIONS, *id.*, at 290. Fried, *supra* note 13, at 205.

21. R.S. Gerstein, *Intimacy and Privacy*, *in* PHILOSOPHICAL DIMENSIONS, *supra* note 8, at 265-71.

22. Gavison, *supra* note 16, at 446-48; MCLEAN, *supra* note 14, at 76.

tual abilities. *Sixth*, privacy is important for the mental health of the individual.[23] In the absence of the capacity to perform acts that are known only to him, a person is forced to continuously conform to social standards, as any deviation from those standards will attract social condemnation. The inhibitions and isolation entailed by this may cause the person psychological harm.

On *the collective level*, privacy plays a critical role in shaping the character of society. True, in the absence of privacy, many wrongful, fraudulent, and hypocritical acts worldwide might not have been committed, and, moreover, the proponents of the communitarian theory question the truth of the liberal ideal to the effect that the individual is an island able to form his personality in isolation from the society in which he lives, and argue that a surplus of privacy impairs his ability to form an independent personality. Yet, the individualistic grounds for privacy make it clear that the essential contribution privacy makes to the formulation of the personal autonomy of the individual, and consequently to the existence of the democratic regime, has a positive value that considerably outweighs its negative aspects.[24] Recognition of the individual as a complex separate entity worthy of respect enables the individual to develop a personality possessing independent moral judgment. A society whose members possess conformist personalities based on submissive acceptance of social norms does not enable the pursuit of the pluralism necessary to create the democratic experience.

When we speak of the legal right to privacy we are referring to the legal protection of privacy. The scope of application of the right envelops the positive aspects of privacy, as these are disclosed by the justifications given for the right. Consequently, to define the legal right to privacy, it is necessary to agree on a definition of the concept of privacy, which will allow us to determine the scope of its application and thereafter its positive aspects.[25] In my opinion, the superior definition is the one that is based on the notion of accessibility, as contrary to the first definition, which is based on the moral importance of privacy but which does not set out what is embraced thereby, and contrary to the second definition, which is based on the notion of control over information but which does not recognize the fact that control is not a guarantee of privacy;[26] this definition eloquently expresses the diverse strands of privacy, which are not necessarily interdependent. When we speak about the *level of secrecy*, we are referring to the public's access to information about the individual (such as accessing his photograph, monitoring his conversations, and data banks that contain information about him); when we talk of the *level of segregation*, we are

23. S.M. Jourard, *Some Psychological Aspects of Privacy*, 31 LAW & CONTEMP. PROBS. 307 (1966); Benn, *supra* note 19, at 241.

24. *See* WESTIN, *supra* note 6, at 23; Benn, *supra* note 19, at 241; Schoeman, *supra* note 8, at 1; Gavison, *supra* note 16, at 443, 449, 455; Y. Livnat, *Individual and Community–Communitarian Criticism of* HCJ 205/94 Nof v. Ministry of Defense, 31(1) MISHPATIM 219, 223-33 (2000) (Heb.).

25. Gavison, *supra* note 16, at 459.

26. Schoeman, *supra* note 8, at 3.

referring to the public's physical access to the individual (such as searches of his body and property); and when we talk about the *level of anonymity*, we are referring to the public directing its attention to the individual (such as through surveillance).

The justifications given for privacy show that neither the complete absence of privacy nor absolute privacy is desirable. It follows that identifying the positive aspects of privacy, i.e., those aspects that should properly be accorded legal protection, requires a balance to be drawn between the two polar extremes mentioned. A balance is not designed in a vacuum, but in the light of the system of values on which the legal system of a particular country is founded.[27] In other words, the greater the commitment of society to the liberal ideal, the more extensive will be the legal protection accorded to privacy and vice versa. A discussion of the appropriate structure of values is outside the scope of this paper; suffice it to say that a proper balance is one that properly reflects a democratic society's commitment to human rights. There is no doubt that in every such balance, factors such as preventing the creation of data banks, preventing filming and monitoring of an individual's conversations, preventing interference with his body and property, and preventing surveillance of his movements, will be regarded as positive and therefore worthy of legal protection.[28]

At the same time, the range of situations falling within the boundaries of the right to privacy is not homogenous, in view of the varying relative weight that may be accorded to the justifications for granting protection in each of those situations.[29] Thus, it may be said that falling within the *core right to privacy* are the situations that lie at the heart of the right because the justifications for including them in the right have the greatest force; consequently, it is anticipated that infringement of privacy in those situations will cause the individual the greatest damage and pain. We are referring here to situations that the individual experiences alone, in the hope that none other than himself knows of them, unless he chooses to reveal them. Situations falling on the *intermediate level of the right* are those where the justifications for including them are weaker, and therefore it is anticipated that an infringement of privacy will cause the individual great pain and damage, albeit less than what he would have experienced had his core right to privacy been affected. The situations we are referring to here are experiences that the individual shares with a small and defined number of other individuals. On the *fringe of the right to privacy* are situations, the inclusion of which can only be justified weakly, and therefore infringement of privacy in those situations will only lead to a low level of pain and dam-

27. Livnat, *supra* note 24, at 243-44.

28. It should be clarified that recognition of the legal right to privacy does not mean that in every case where the right clashes with other rights and interests it will override. Recognition of the right is only an essential preliminary condition for its identification as a relevant element in situations where it clashes with other rights and interests and where, therefore, a need arises to draw a balance between all the interests. For further elaboration of this point, see Gavison, *supra* note 16, at 467.

29. Benn, *supra* note 19, at 234; R. A. Wasserstorm, *Privacy: Some Arguments and Assumptions*, in PHILOSOPHICAL DIMENSIONS, *supra* note 8, at 317.

age to the individual. These situations are experiences that the individual shares with a large, but defined, number of other individuals.

B. The National Security Interest

The path described in relation to the right to privacy will now be applied to the discussion concerning the substance of the national security interest. The concept "national security," like the concept "privacy," is amorphous and devoid of precise analytical meaning. Its scope of application is not limited solely to situations in which the state defends itself against an illegal domestic or foreign threat of force to its institutions or to the people present within its borders, even though this is the heart of the concept. Rather, it embraces a range of situations that influence the ability of the regime to effectively pursue the collective welfare of the nation.[30] Thus, for example, while at the periphery of the concept one may find governmental actions in the spheres of education and transport, at its core one may find military war-like acts and anti-terrorist activities.

National security is a public resource, the justifications for which are readily understood, because there is no more essential collective national goal than preserving national security, safeguarding the lives of the citizens and ensuring public order.[31] Security is an essential condition for achieving these objectives, and without it no significance can be attached to human rights and the other individual and collective interests.[32]

The national security interest delineates the scope of the legal protection of national security and embraces the security aspects for which justification is found on national security grounds. Contrary to privacy, absolute security is the utopian ideal, and therefore "national security" as a whole is worthy of legal protection[33] in the sense that the state has the duty and the right to protect itself and the persons who are located within its borders against security threats.[34] In this paper I shall confine myself to one of the core aspects of the security interest—that which deals with the duty and the right of the state to protect itself against domestic and foreign terror attacks.[35]

---

30. T.I. Emerson, *National Security and Civil Liberties*, 9 YALE J. WORLD PUB. ORD. 78, 79 (1982).

31. G. Barzilai, *Center Versus Periphery: "Anti-Terrorist Laws" as Politics*, 8 PLILIM 229, 230 (2000) (Heb.); Emerson, *supra* note 30, at 80.

32. I. Zamir, *Human Rights and National Security*, 19 MISHPATIM 17 (1989) (Heb.).

33. These comments are made by way of analogy to the analysis offered by Professor Gavison in relation to the right to privacy. *See* Gavison, *supra* note 16, at 440, 459.

34. Assa Casher, MILITARY ETHICS 37-39 (3d ed. 1998) (Heb.).

35. Many definitions have been given to the word "terror"; however, none are incisive and authoritative. For the purpose of this discussion we may be satisfied with use of the term to describe the deliberate performance or threat of performance of acts of physical violence or menacing persons who are not combatants, to achieve any particular purpose, generally a political goal. Law enforcement bodies which lawfully employ force to maintain public order and random acts of violence do not comprise acts of terror, even though formally speaking they may fall within certain of its elements. For a discussion about the nature of terror and who is a terrorist, see E. Gross, *Legal Aspects of Tackling*

C. The Right to Privacy Versus the National Security Interest

A key condition for conducting an intelligent discussion of these issues is an understanding of the fundamental concepts involved therein. As the concepts of privacy and national security are difficult to define, there is an inherent risk that they will be perceived on an intuitive non-rational level, which will undermine the ability to conduct a pertinent discussion of the proper balance that should be drawn between these values in the event of a clash.[36] Thus, when on one hand we are witnesses to concrete atrocities, scenes of streets and malls transformed into arenas of death, and on the other we are faced with an abstract right, our intuition tilts the balance unequivocally in favor of national security. To enable a discussion of the legal and moral aspects of the proper balance between the right to privacy and the national security interest, in so far as relates to the war against terror, the two earlier subsections were devoted to a clarification of these concepts.

At this point I shall turn to an examination of the ways in which the right to privacy may be infringed.

II. Means of Infringing the Right to Privacy

If, in the beginning of the 20th century, there were those who believed that there was nothing left to invent,[37] the technological developments of this century proved to the skeptics that mankind remains engaged in the incessant pursuit of boundless innovations and inventions. The further our progress in this pursuit, the more aware we become that those innovations that improve the quality of our lives also have the potential to interfere with areas of our life that were once inaccessible to anyone but ourselves. Knowledge of what is being done in these spheres of life, in so far as they are exploited to plan acts of terror, is often what enables us to foil these terrorist acts. However, the situation is much more complex than it seems because identifying the areas of life relevant to terrorism entails interfering with the privacy of the entire public. How can we catch a terrorist carrying an explosive belt without x-raying the bodies of all passengers on a plane? How can we uncover a terrorist cell whose members communicate via electronic media, without uncovering the contents of their communications and at the same time scanning the innocent communications of millions of people? And how should we identify a terrorist collecting intelligence regarding security procedures in a tourist site or shopping mall, without placing surveillance cameras that not only film suspicious activities but also the activities of innocent people?

Terrorism: The Balance Between the Right of a Democracy to Defend Itself and the Protection of Human Rights, 6 UCLA J. INT'L L. & FOREIGN AFF. 89, 97-101 (2001).

36. MCLEAN, *supra* note 14, at 3; Zamir, *supra* note 32, at 18.

37. In 1899 Charles Duell, the U.S. Commissioner of Patents, argued that "[e]verything that can be invented has been invented." *See* W. Isaacson, *Who Mattered and Why*, *at* http://www.time.com/time/time100/poc/magazine/who_mattered_and_why4d.html (last visited July 27, 2003).

A. Human Detectives

Privacy may be invaded in a wide variety of ways. Human detectives have been at work since time immemorial.[38] There are clear benefits to be gained by surveillance of the activities of a person suspected of terrorist activities, searching his person and property (sometimes with the aid of dogs trained to sniff out explosives), interrogating those in contact with the suspect, and maintaining proximity to eavesdrop into his conversations. Yet, the limitations inherent in human surveillance—the fact that it entails the allocation of enormous human and economic resources, the fact that it is dependent on the skills and expertise of the persons performing the surveillance, and the difficulty in disguising the trackers and the risks they face—has led over the years to a decrease in the use of individuals and greater reliance on technological surveillance measures.[39]

B. Technological Surveillance Measures

Technological surveillance measures may be divided into five categories:

1. *Technologies for Scanning Communications*

Visual surveillance is carried out by positioning closed circuit television cameras in public places (such as on the street or at bus stops) or in private places (such as in houses and vehicles), which relay live pictures to a control center. Advances in optical technologies have resulted in sharper picture resolution and night time pictures that resemble daylight pictures in quality, thereby enabling the control center team to carry out close proximity filming of suspicious articles.[40] Visual documentation has multiple advantages, including assisting the identification of terrorists seeking an "ideal" place to carry out a suicide bombing or conceal an explosive package as well as spot collaborators engaged in collecting intelligence for future terrorist attacks. Likewise, documentation produced during the occurrence of a "successful" terrorist event enables the security forces to determine the nature of the security flaws, which can then be rectified so as to avoid similar future attacks. *Audio surveillance* is carried out by means of audio tape devices or telephone taps.[41] *Electronic wiretapping*

38. N. Rakover, *Protection of Privacy* 17, *in* 4 SERIES OF STUDIES AND REVIEWS IN JEWISH LAW (Ministry of Justice 1970).

39. L.D. Sloan, *Echelon and the Legal Restraints on Signals Intelligence: A Need for Reevaluation*, 50 DUKE L.J. 1467, 1474 (2001); M.G. Young, *What Big Eyes and Ears You Have! A New Regime for Covert Governmental Surveillance*, FORDHAM L. REV. 1017, 1035 (2001).

40. C. Slobogin, *Symposium: Public Privacy: Camera Surveillance of Public Places and the Right to Anonymity*, 72 MISS. L.J. 213, 219-22 (2002).

41. Apart from eavesdropping into the content of telephone conversations, it is possible to tap identifying details, i.e., to record the telephone numbers dialed from a particular telephone number (by means of a device known as a pen register), the telephone numbers calling in (by means of a trap and trace device), as well as the time and duration of the call. *See* Young, *supra* note 39, at 1024-32; 1 C.S. FISHMAN & A.T. MCKENNA, WIRETAPPING AND EAVESDROPPING 5:11 at 5-15, 5-16 (2d ed. 1995).

can be carried out by a range of devices. In relation to the internet, the best known tool is the American Carnivore program, which is able to scan the internet transmissions of all the subscribers of a provider upon whose server the program is installed and register identities (i.e., record the internet sites visited by the surfer, the email addresses of the surfer, and those of his contacts) as well as register the content (record the activities of the surfer in the internet sites visited by him—such as purchases at a public online auction, information sought using a search engine, and the contents of his communications) of transmissions that fall within certain defined parameters.[42] Scanning internet transmissions enables the security authorities to track individual terrorist suspects, as well as to engage in more general surveillance aimed at identifying user practices or cyber communications characteristic of terrorists. However, a terrorist who is aware of the possibility of electronic tapping can adopt a variety of measures to camouflage his activities, such as using encryption programs that convert his electronic communications into indecipherable code.[43] All the addressee need do is tap in the password of the appropriate decoding program while the security authority is forced to try and breach the encryption program—a complex and time-consuming process that is often impossible. The solution to this problem is a program installed on the computer of the sender or receiver of the communication, which records all the key strokes typed by someone using an operating computer (including the password of the encryption program) and then sends the information to a defined email address. Installation of the program (known as Key-Logger) may be performed manually—which requires physical access to the computer—or by means of a virus (known as Magic Lantern) that is operated when a person opens an email attachment or visits a certain site.[44]

Reports that have not yet been officially confirmed also tell of the existence of an intelligence gathering project known as Echelon, which scans all the types of electronic communications described above and filters and records information meeting particular parameters.[45]

---

42. The Carnivore program underwent three rhetorical cycles: the FBI began developing it in 1997 under the name "Omnivore" (eater of everything); in 1999 the name was changed to "Carnivore" (meat eater); however, because both names had an immediate negative connotation, in 2001 the program was given a neutral technical name—Digital Collection System 1000 (DCS-1000). Since Carnivore was the name which took hold in the public mind, I too shall refer to the program in that way. T.R. McCarthy, *Don't Fear Carnivore: It Won't Devour Individual Privacy*, 66 Mo. L. Rev. 827, 827-35 (2001); K.A. Horn, *Privacy Versus Protection: Exploring the Boundaries of Electronic Surveillance in the Internet Age*, 29 Fordham Urb. L.J. 2233, 2234-36 (2002).

43. J.T. Stender, *Too Many Secrets: Challenges to the Control of Strong Crypto and the National Security Perspective*, 30 Case W. Res. J. Int'l L. 287, 293-97 (1998).

44. A. Nance, *Taking the Fear Out of Electronic Surveillance in the New Age of Terror*, 70 UMKC L. Rev. 751, 755-57, 768-70 (2002).

45. According to reports, the project is being operated by the United States, England, Canada, Australia, and New Zealand. Sloan, *supra* note 39, at 1470-72.

2. *Technologies for Enhancing the Quality of Information Obtained by Natural Senses*

Normal enhancement refers to information that the human senses are capable of discerning without technological assistance (for example, binoculars, telescopes, night vision glasses and satellite photographs improve the quality of information obtained visually), whereas abnormal enhancement refers to information that the human senses are not capable of discerning without technological assistance.[46] Thus, metal detectors enable the detection of metal weapons concealed under clothing or in baggage. The thermal imager detects the infrared heat waves emitted by every object and presents them as a visual image colored according to the degree of heat of the object, while advanced devices are even able to detect heat waves through closed walls.[47] It is possible to make use of this imager not only to detect traditional weapons and explosives on the body or in the property of a person but also when rescuing hostages, as it is capable of revealing the location of the terrorists and their physical condition at any given moment. The passive millimeter wave imager detects electromagnetic radiation naturally emitted by objects and presents them as high resolution images, which, inter alia, allow the contours of a person to be detected through his clothes or baggage (such as weapons or explosives but also pens and coins).[48] The radar skin scanner produces even more precise images, which allow any object larger than a millimeter to be detected and consequently reveal the most intimate details of a person.[49] Likewise, a broad range of x-ray cameras image the naked body of a person through his clothes at different levels of resolution, the most advanced of these cameras providing an image that leaves no room for the imagination.[50] At the same time, these devices may be equipped with accessories that reduce the degree of infringement to a person's privacy, such as accessories that distort the face of the subject or systems that are programmed not to show the operator an image save if it detects items that have the shape of weapons or explosives.[51]

3. *Technologies for Mapping Location*

An electronic tracking device, generally called a beeper, is a miniature radio transmitter that broadcasts signals on a cyclical basis. The signals

46. T.W. McKnight, *Passive, Sensory-Enhanced Searches: Shifting the Fourth Amendment "Reasonableness" Burden*, 59 LA. L. REV. 1243 (1999).

47. *Id.* at 1249; Young, *supra* note 39, at 1033-34.

48. A.L. Rosenberg, *Passive Millimeter Wave Imaging: A New Weapon in the Fight Against Crime or a Fourth Amendment Violation?*, 9 ALB. L.J. SCI. & TECH. 135, 138-40 (1998).

49. A.M. Froomkin, *Symposium: Cyberspace and Privacy: A New Legal Paradigm? The Death of Privacy?*, 52 STAN. L. REV. 1461, 1500 (2000).

50. *Id.*; transcript of an interview with David Sobell and John Mica, aired on June 26, 2003, *at* http://edition.cnn.com/TRANSCRIPTS/0306/26/se.02.html (last visited July 27, 2003).

51. *Id.*; S.S. Flores, *Gun Detector Technology and the Special Needs Exception*, 25 RUTGERS COMPUTER & TECH. L.J. 135, 139 (1999).

are received by a compatible device, which maps its location and consequently the movements of the object in which it is placed. So long as the beeper remains within the range of the mapping device, the tracked object cannot be lost. In cases where the beeper moves out of range, it is easier to relocate it than in the case of physical tracking.[52] Technologically more sophisticated tracking procedures enable the operator to ascertain the location of a person by means of the cellular telephone he carries, by mapping the cyclical signals broadcast by every cellular telephone linked to a communications network.[53]

4. Identification Technologies

Identification technologies such as passwords and magnetic cards are not reliable means of identifying people, as these can be borrowed or stolen.[54] Biometric measures, however, identify the individual on the basis of unique non-transferable physical characteristics.[55] Thus, *DNA fingerprinting*[56] allows the molecular structure of a person to be identified and then converted into a digital code. This technique is highly reliable[57] because apart from identical twins, each person has a unique DNA fingerprint. With *retinal scanning*[58] a light beam scans the blood cells in the eye and converts the data into a digital code. Because the retina undergoes almost no natural changes during the course of a person's life, this technique is regarded as extremely accurate. Nonetheless, inaccuracies may be caused by changes in the blood vessel structures resulting from trauma or disease. *Iris recognition*[59] refers to the process of scanning the structure of the iris using a video camera. This system too is highly reliable, as the structure of the iris remains the same over time. *Fingerprinting*[60] requires a person to place his fingers over an optical scanner. This system is highly reliable, although inaccuracies may be caused by dirt left on the scanner from previous use or by changes to the structure of the fingers (caused by scratches or cuts that have left scars or prolonged manual labour) or by reason of deliberate trickery (spreading clear adhesives that distort the structure of

52. C.S. Fishman, *Electronic Tracking Devices and the Fourth Amendment: Knotts, Karo and the Questions Still Unanswered*, 34 CATH. U. L. REV. 277, 281-82 (1985).

53. Froomkin, *supra* note 49, at 1479-80; M.M. Werdegar, *Lost? The Government Knows Where You Are: Cellular Telephone Call Location Technology and the Expectation of Privacy*, 10 STAN. L. & POL'Y REV. 103, 105-06 (1998).

54. J.D. Woodward, *Biometric Scanning, Law and Policy: Identifying the Concerns–Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 101 (1997).

55. *Id.* at 99-101.

56. R.S. Peterson, *DNA Databases: When Fear Goes Too Far*, 37 AM. CRIM. L. REV. 1219, 1222-23 (2000).

57. The accuracy and reliability of a biometric device is determined according to two parameters. First, the proportion of false identifications (the number of cases in which a person whose details have not been scanned into the system is identified as a person whose details have been scanned). Second, the proportion of false rejections (the number of cases in which a person whose details have been scanned into the system in the past is not identified by it). *See* Woodward, *supra* note 54, at 101.

58. *Id.* at 102-03.

59. *Id.* at 103-04.

60. *Id.* at 104-05.

the fingers). *Hand geometry*[61] requires scanning of the length, width, and height of the hand using an optical scanner. This technique has a low level of reliability, as over the years, the palm of the hand undergoes many changes—whether from aging, injuries, or carrying heavy loads. *Face recognition*[62] requires photographs to be taken of a person's face, following which a computer program measures angles and distances between geometrical points on the face. This technique too possesses only a low level of reliability because it finds it difficult to distinguish between people possessing similar facial structures and is easily influenced by alteration of the angle of photography or modifications to the person's external appearance (such as growing or removing a beard). *Voice recognition*[63] requires the recording and measurement of the frequency and pitch of a person's voice. This technique possesses a low degree of reliability as a person's voice alters with age, during illness, in times of strong emotion, or as a result of background noise. In *signature recognition*,[64] a computerized system records the manner in which a person shapes letters, the speed of writing, the pressure placed on the page, and the number of times that the writer has raised his hand from the page. Injury or deliberate arbitrary movements easily change the manner of writing, making this technique highly inaccurate.

The range of techniques described above follow an identical process.[65] First, each system scans the characteristic on which it focuses. During the second stage, the data is converted into a digital code. Subsequently, the code is entered into a computerized data bank that contains other codes entered in the past. Finally, the system engages in identification or verification of identity. The first function involves scanning the details of a person whose identity is unknown and then comparing the data to all the codes contained in the data bank in the hope of finding a match. The second function involves scanning the details of a person claiming a particular identity and thereafter comparing those particular details to the code of the person whose identity has been claimed, in an effort to find a match and thereby verify his claim. The characteristics on which the biometric techniques focus have the potential to reveal information concerning the health of the person. Thus, for example, the human genome reveals information concerning a predisposition to contract a particular disease; the structure of the iris and the retina point to the possible existence of diseases such as diabetes, high blood pressure, and AIDS, and certain studies claim that the

61. *Id.* at 105-06.

62. D. McCormack, Note, *Can Corporate America Secure Our Nation? An Analysis of the Identix Framework for the Regulation and Use of Facial Recognition Technology*, 9 B.U. J. SCI. & TECH. L. 128, 131 (2003); feature on FACE RECOGNITION, Publication of the American Civil Liberties Union, *at* http://www.aclu.org/privacy/privacy.cfm?ID=12119&c=130 (last visited July 27, 2003).

63. R. Moo-Young, *Eyeing the Future: Surviving the Criticisms of Biometric Authentication*, 5 N.C. BANKING INST. 421, 435 (2001).

64. *Id.* at 435-36.

65. L.J. McGuire, *Banking on Biometrics: Your Bank's New High-Tech Method of Identification May Mean Giving Up Your Privacy*, 33 AKRON L. REV. 441, 445 (2000).

geometrical structure of the hand points to the sexual orientation of a person and his predisposition to chromosomal disorders. Accordingly, the important question arises whether, after the biometric characteristic has been converted into a digital code, obstacles should be placed on examining this information or whether the system should still allow it to be analyzed.[66]

The biometric systems are of great importance in the fight against terrorism, as these can be positioned at the entrances to security sites or at sites containing dangerous materials, such as fuel and gas depots, to prevent terrorists from infiltrating and carrying out mega attacks. Likewise, they can be positioned in public places to locate known terrorists whose details have already been scanned into the system. They may be enhanced by integrating them in systems belonging to other categories. Thus, for example, a voice recognition system integrated with a system for intercepting telephone calls would significantly increase the likelihood of intercepting conversations between terrorists. Similarly, a face recognition system combined with a closed circuit television data bank would make it easier to locate wanted persons.[67]

5. *Technologies for Integrating Information*

Information collected using the measures described above, like information gathered from other sources, may be recorded and stored in computerized data banks. Uniting these data banks into a super data bank enables the compilation of a detailed portrait of the habits and lifestyle of the subject.[68] Thus, for example, uniting data banks managed by governmental authorities (such as registries of criminal records, family status, education, and health) with data banks managed by private business enterprises (such as financial registries, telephone records, public library lending records, and records of searches and purchases at public online auctions), would create a central data bank that would allow the identification of persons whose actions or lifestyles are characteristic of terrorists or supporters of terrorist organizations.[69]

6. *Terrorism profiling*

Because good management of popular public places precludes the stringent application of the measures described above to all those entering

66. Froomkin, *supra* note 49, at 1495; Woodward, *supra* note 54, at 115-16; Peterson, *supra* note 56, at 1223.

67. Sloan, *supra* note 39, at 1481; C.S. Milligan, *Facial Recognition Technology, Video Surveillance and Privacy*, 9 S. CAL. INTERDISC. L.J. 295, 306 (1999).

68. J. STANLEY & B. STEINHARDT, BIGGER MONSTER, WEAKER CHAINS: THE GROWTH OF AN AMERICAN SURVEILLANCE SOCIETY 3-4, Publication of the American Civil Liberties Union, *at* http://www.aclu.org/privacy/privacy.cfm?id=11573&c=39 (last visited June 2, 2003).

69. The best known initiative to establish a super data bank was that taken by the US Department of Defense to create the TIA (Total Information Awareness). Certain repugnance for this name caused it to be changed to Terrorism Information Awareness. *See* http://www.darpa.mil/body/tia/TIA%20ES.pdf (last visited July 27, 2003).

the premises, and because taking security measures entails significant costs, it has become increasingly necessary to shift from zeroing in upon individual terrorist suspects to locating suspect groups, the members of which are subject to much more stringent scrutiny than the rest of the public.

Terrorist profiling operates in a three-stage process.[70] In the *first stage*, the intelligence services collect the maximum amount of data about known terrorists (their country of birth, gender, age, family status, socio-economic status, religious affiliation, religious commitment, education, lifestyle, etc.). Next, a statistical analysis is carried out by determining the frequency of each of the data and establishing the most frequent characteristics as the criteria for the profile of the potential terrorist. People fitting these criteria are regarded as being more likely to be terrorists than people who do not fit the criteria. In the *second stage*, methods are established for identifying the people who fit the profile. While most of the details regarding the process of identification are secret, it may be said that they are based both on a subjective test that examines the behavior of the person in the relevant situation (nervousness, sweating, impatience, dishevelment, or excessive neatness, etc.) and on an objective test that examines factors that are independent of behavior (such as gender, age, nationality, religion, skin color). In the third stage, those found to comply with the profile are subjected to prolonged and stringent investigative processes, which include interrogations and searches of their persons and property.

Profiling is used in four situations. The most well-known and common situation is the profiling of passengers at sea ports and in airports (passenger profiling). In 1931, the first plane hijacking took place, when Peruvian revolutionaries took control of an airplane to distribute propaganda leaflets to residents of the country. In 1949, the first terrorist caused a commercial aircraft to crash, when a woman hired two released convicts to hide a bomb in a Philippines Airlines aircraft in which her husband was to fly. Six years later, the United States suffered the same experience when a passenger boarded a plane without knowing that his luggage contained a bomb planted by his son, who had plotted to kill him to obtain payment from his father's life insurance.[71]

These events showed the world the enormity of the catastrophe that could occur in sea and air transport, and indeed they formed only the first three links in a lengthening chain of terrorist and hijacking activities that continue to this day. The efforts by a number of countries to eradicate this phenomenon led to the invention of a variety of safety measures, which included, inter alia, variations on the profiling system. Thus, for example, the American airline companies feed the profile criteria into a computerized system known as CAPPS (Computer Assisted Passenger Prescreening System), which picks out passengers possessing suspect characteristics

70. D. Smith, *Passenger Profiling: A Greater Terror than Terrorism Itself*, 32 J. MARSHALL L. REV. 167, 168-72 (1998).

71. J.H. Daniel, *Reform in Airport Security: Panic or Precaution?*, 53 MERCER L. REV. 1623, 1624-25 (2002).

from data banks operated by the airline companies containing the personal details and destinations of their customers. Passengers fitting the profile, together with a random sample of incompatible persons, are required to undergo stringent and prolonged interrogative and examination procedures. The possibility of upgrading the system by adding a large number of private data banks (such as records of credit card purchases and purchases at online public auctions) and public data banks (such as criminal records and data banks operated by the intelligence services) is currently being discussed.[72]

A small group of people, who are more strongly suspected of involvement in terrorist activities, is exempt from the profiling system described above because their names in any event appear on the "No-Fly List" operated by the FBI. These people require particularly lengthy and rigorous investigation, at the end of which they are not always allowed to fly.[73]

In relation to Israeli airline companies, during the baggage check-in, prior to receiving a boarding card, every passenger is asked a short series of questions (such as to whom the suitcases belong, who packed them, when and where the packing took place, where the suitcases were kept between the completion of packing and arrival at the check-in, and whether the passenger had been asked to carry anything for anyone). These questions are designed to give the security staff time to determine whether the passenger fits the profile criteria, based on the subjective parameters described above as well as objective parameters, such as the method of payment (cash or credit), whether the passenger has arrived alone or is accompanied by another, places of departure and destination, whether the air ticket is a single or return, whether the ticket was purchased in advance or proximate to the time of departure, whether the passenger plans to hire a vehicle in the country of destination, etc.[74] As in the United States, a defined group of passengers is exempt from this process because the names of these passengers appear on the border control list operated by the General Security Service, subjecting them to much more rigorous security processes.[75]

The second situation in which profiling is used is upon entry into public places (the checks conducted of persons entering places such as restaurants and bus stations, for example). These are much less thorough than those conducted in the ports and are chiefly based on subjective behavioral characteristics and objective data such as external appearance, sometimes aided by information drawn from various data banks.

---

72. E. Baker, *Flying While Arab-Racial Profiling and Air Travel Security*, 67 J. AIR L. & COM. 1375, 1379 (2002); DATA PROTECTION SINCE 11 SEPTEMBER 2001: WHAT STRATEGY FOR EUROPE?, Publication of Electronic Privacy Information Center, *at* http://www.epic.org/privacy/intl/ep_statement_032503.pdf (last visited 3 August, 2003).

73. Press Release, American Civil Liberties Union, Government Agency Releases Documents on NO FLY, List, *at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=13193&c=206 (last visited Aug. 3, 2003).

74. L. Braber, *Korematsu's Ghost: A Post September 11th Analysis of Race and National Security*, 47 VILL. L. REV. 451, 460-61 (2002).

75. H.C. 4950/90 Tikvah Franz et al. v. Minister of Defense et al., 47(3) P.D. 36.

The third situation concerns profiling of passersby (such as responding to security alerts about the infiltration of terrorists or as part of routine security measures); the security forces place road barriers and patrol city streets with the object of delaying, questioning, and sometimes even searching the persons, vehicles, and property of people fitting the profile criteria, where the identification procedure is based on identifying suspect behavior, external appearance, possession of a vehicle suspected of being stolen, or carrying non-Israeli license plates and the like.

The fourth situation in which the profile is used has an investigative purpose as well as a preventive purpose in that it relates to profiling subsequent to a terrorist attack. Following every terrorist incident the security forces not only question witnesses but also detain for interrogation or arrest persons found at the site of the attack (including, on occasion, people who themselves have been injured) or people seen in the vicinity shortly after the attack, if they conform to the profile of persons suspected of involvement in the incident.[76]

As noted in the previous section, not all the circumstances falling within the right to privacy are uniform in nature. Accordingly, we must consider the degree of harm that each of the measures described above causes to the right, based on the standards described in the last section. *Violation of the core right to privacy* occurs when body searches are conducted, when the suspect is x-rayed and his biometric fingerprints are taken, thereby revealing his medical information. *Violation of the intermediate level of the right* occurs when events occurring at the home of the suspect are recorded, searches are conducted of his premises or property, his friends are questioned, his conversations monitored, his movements in private places are tracked, and a range of biometric fingerprints, which do not reveal medical information, are taken from his person. *A violation at the fringes of the right* occurs when a person's acts and movements in public places are tracked and recorded. Data banks can contain information belonging to each facet of the right, and therefore it is the content of the information located in each data bank that dictates the gravity of the violation.

If, in the past, George Orwell's ominous prophesy concerning "Big Brother" tracking and recording every facet of the lives of the populace was regarded as unrealistic because of the technological impossibility of actualizing that goal, the above remarks show that today we live in a society in which there is no such impediment. The issue of the restrictions that a state in fact sets for itself and those that it should properly set for itself—when required to safeguard state security yet continue to preserve the privacy of its citizens—is the subject of the next section.

76. T. Rotem, *First the Shock of the Explosion, Afterwards the Fear that They Will Think that I Am a Terrorist*, HA'ARETZ, Sept. 29, 2002.

III. The Legal Situation in Israel

In 1966, Israel signed the International Covenant on Civil and Political Rights, which provides in Article 17 as follows:

> 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 protection of the law against such interference or attacks.[77]

In Israeli domestic law, recognition of the right to privacy was initially implied from a line of statutory provisions that qualified the right to search the person and premises of the individual, enter his property, disseminate information about him, etc. However, over the years, as the methods of invading a person's private life grew in quantity and sophistication, the force of the traditional protections eroded and statutes were enacted that entrenched various aspects of the right to privacy, such as protection against monitoring and human and electronic surveillance.[78]

When Basic Law: Human Dignity and Freedom was adopted in 1992, its contribution to the protection of privacy was twofold. First, privacy was recognized as an integral part of the human right to dignity, and therefore it was granted the status of a constitutional basic right, which every governmental authority must respect.[79] Second, for the first time, a statute entrenched a *general* right to privacy—not one confined to the specific issues that up to then had been established by statute.[80] At the same time, because the concept of privacy was incapable of exhaustive definition, the courts found it difficult to clearly delineate the boundaries of the right and satisfied themselves with a general statement of principle:

---

77. The Covenant was signed by Israel on December 19, 1966, ratified on August 18, 1991, and entered into force on January 3, 1992. *See* International Covenant on Civil and Political Rights, 999 U.N.T.S. 171. A similar provision is found in Article 12 of the Universal Declaration of Human Rights, to the following effect: "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks." *See* Universal Declaration of Human Rights (1948), *at* http://www.hrweb.org/legal/udhr.html (last visited August 3, 2003). For the legally binding nature of the Declaration, *see* I. Brownlie, PRINCIPLES OF PUBLIC INTERNATIONAL LAW 572 (Clarendon Press, 3d ed. 1979).

78. Protection of Privacy Bill - 5741-1980, Hatzaot Chok 1453 at 206; R. Gavison, *The Right to Privacy, in* HUMAN AND CIVIL RIGHTS IN ISRAEL 303, 308 (T. Ben-Gal et al. eds., vol. C 1992).

79. Section 11 of Basic Law: Human Dignity and Freedom, 1992, S.H., 150; A. Barak, *Interpretation in Law* 421 (vol. 3: CONSTITUTIONAL INTERPRETATION, 1994).

80. Section 7 of Basic Law: Human Dignity and Freedom provides as follows:

> (a) All persons have the right to privacy and to intimacy.
>
> (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 his body or personal effects.
>
> (d) There shall be no violation of the confidentiality of conversation, or of the writings or records of a person.

> Now, as it has been given an enacted constitutional basis, it must be interpreted from a "wide perspective" . . . and out of an understanding that we are concerned with a provision which establishes a way of life. We are concerned with human experience which must conform itself to a changing reality . . . accordingly a constitutional provision must be interpreted from a broad perspective and not in a technical manner . . . applying a substantive approach and not a legalistic approach . . . applying a pertinent approach and not a technical or pedantic approach . . . the right to privacy draws the line between the individual and the public, between the "self" and society. It delineates a zone in which the individual is left to himself, to develop his "self," without the involvement of others.[81]

It follows that despite the general difficulty in determining the precise scope of application of the right, it clearly contemplates protection of the individual against the use of measures of the type described in the preceding section.

It has been recognized that even in places where the human right to privacy does apply, the legal protection of that right is not absolute, and there will be cases where the right will be superseded by more important interests, including the public interest in national security:

> Doubtless, when we come to interpret statutory provisions we shall take into account the fact that the right to privacy is an important right, but we are not exempt from an examination of all the relevant factors and values, only the weighing of which, within the framework of the statutory provision, can lead us to the requisite outcome under the law.[82]

The relativism of the right to privacy, like the relativism of all human rights, ensues from the individual's obligation to sacrifice his rights for the benefit of the community in which he lives, to the extent necessary to ensure its continued existence, since that existence is a prerequisite to his ability to actualize his rights.[83] Sacrificing these rights is only constitutional if it is carried out by virtue of a valid law that is compatible with the values of the State of Israel as a Jewish and democratic state, it has a proper purpose, and where the extent of the violation of the right does not exceed what is necessary.[84]

There is no doubt that a violation of privacy aimed at preventing a terrorist attack on innocent people has a worthy purpose that accords with the values of Judaism and democracy, both of which recognize the necessity of reducing standards of protection of individual rights in times of crises and emergency, as opposed to times of peace and tranquility, to enable the state to provide effective protection against threats to it.[85] Consequently, the primary problem centers on the extent to which these stan-

---

81. H.C. 2481/93 Dayan v. Superintendent of the Jerusalem District, 48(2) P.D. 456, per Barak, *supra* note 79, at 470 (Heb.).

82. H.C. 3815/90 Gilat v. Minister of Police, 45(3) P.D. 414, 423 (Heb.).

83. Z. Segal, *The Right to Privacy Versus the Right to "Know,"* 9(1) IUNEI MISHPAT 175, 176 (1983) (Heb.).

84. Section 8 of Basic Law: Human Dignity and Freedom, *supra* note 79.

85. H.C. 680/88 Schnitzer v. The Chief Military Censor, 42(4) P.D. 617, 630 (Heb).

dards must be reduced, i.e., finding the line that separates constitutional violations of privacy from violations that exceed what is necessary.

The case law has held that finding this line entails a threefold test.[86] (A) *The compatibility test*—the infringing measure must lead rationally to the achievement of the purpose of the infringement. (B) *The least harm test*—among all the measures suitable for achieving the purpose, the selected measure must be the one that causes the least harm to the right. (C) *The proportionality test*—there must be a reasonable relationship between the benefit accruing from realizing the purpose and the damage caused to the individual as a result of the violation of his constitutional right.

When we seek to determine whether violations of privacy satisfy these conditions, we must take into account the basic premises underpinning democratic society: on one hand, the war against terrorism does not justify abandoning basic values in every case where a privacy violation would assist the state. Even in its most difficult times, society must adhere to the values for which it is fighting. On the other hand, notwithstanding that human rights require democracy to struggle with one hand tied afore, those rights are not a springboard for national ruin.[87] Accordingly, national security will enable proportional violation of human rights for the sake of those human rights and to ensure their continued preservation. We are referring here to a vertical constitutional balance that accords priority to the public interest in security over human rights, upon satisfying a probability test that case law has not yet definitively determined.[88] There are those who believe that only a near certainty of real harm to national security justifies a violation of human rights, while others are satisfied with the reasonable likelihood test.[89] In view of the special unremitting character of the struggle faced by Israel, I agree with the following comments of Professor Aharon Barak, the President of the Israeli Supreme Court:

> These formulations are good when there are special concrete and specific dangers, within the context of defined events. It is not possible to turn to them when we are concerned with social phenomena which form part of a continuous process. In this matter broad margins of security must be maintained, as it is not possible to take unnecessary risks . . . at the same time . . . we must not accept a probability test which is satisfied solely with a distant risk. It seems to me that the proper balance will be found in the reasonable likelihood test.[90]

---

86. Barak, *supra* note 79, at 536.

87. A. Barak, *Comments at the Opening of the Legal Year 2002*, 16 LAW AND ARMY 1, 2-5 (2002) (Heb.).

88. H.C. 2481/93 Dayan v. Superintendent of the Jerusalem District, 48(2) P.D. 456, 475.

89. Election Appeals [E.A.] 2/84 Neiman v. Chairman of the Central Elections Committee of the Elections to the Eleventh Knesset, 39(2) P.D. 225, 311 (Heb.).

90. *Id.*

Based on the foregoing, I shall now turn to an examination of the scope of the protection accorded by Israeli law to the right to privacy, in cases where it clashes with the national security interest.

A. Security Searches

Israeli law permits searches to be conducted of the premises of a person, as well as of his body and his personal effects, for a variety of purposes. The general arrangement regarding the power to search premises provides that a police officer is entitled to conduct a search in a house or place without a warrant if the following apply:

1. He has reason to believe that a felony is being committed, or has recently been committed therein;

2. The occupier thereof calls in the assistance of the police;

3. Any person therein calls in the assistance of the police, and there is reason to believe that an offence is being committed therein;

4. He is pursuing a person evading arrest or escaping from lawful custody.[91]

In every other case, a search may only be conducted with a warrant, which a judge has discretion to grant in the event of one of the following:

1. A search of the house or place is necessary to secure the production of any article for the purpose of any investigation, trial or other proceeding;

2. The judge has reason to believe that the house or place is used for the deposit or sale of a stolen article, or that there is kept or deposited therein any article by means of or in respect of which an offence has been committed or which has been used, or is intended to be used for any illegal purpose; or

3. The judge has reason to believe that a crime has been committed or it is intended to commit an offence against a man present therein.[92]

Regarding body searches, even though these violate the individual's core right to privacy, the searches themselves are distinct in terms of their degree of gravity: a search of the stomach contents of a person is distinct from a search of his clothes. Accordingly, the law distinguishes between three types of searches:[93] the *most invasive type*, defined as an "internal search," is carried out by blood tests, imaging of the interior of the body using supersonic devices, x-rays, ultrasounds, or gynecological examinations. The *intermediate* test, defined as an "external search," is carried out

91. Section 25 of the Criminal Procedure (Arrest and Searches) Ordinance (New Version) 5729-1969, N.V. 12, 1969 284 (hereinafter the Criminal Procedure Ordinance).

92. Section 23 of the Criminal Procedure Ordinance, *supra* note 91.

93. Section 22 of the Criminal Procedure Ordinance, *supra* note 91; Section 1 of the Criminal Procedure (Powers of Enforcement—Searches of the Body of the Suspect) Law 5756-1996, S.H. 1573 136 (hereinafter the Criminal Procedure Law). It is important to note that, subject to a number of exceptions, a search may only be conducted by someone of the same gender as the suspect. *See* Section 46 of the Criminal Procedure Law; Section 2 of the Criminal Procedure Law; Criminal Applications [Cr. Applic.] 2145/92 State of Israel v. Guetta, 56(5) P.D. 704, 713-14 (Heb.).

by a frontal examination of the naked body of a person; fingerprinting all aspects of the body; removing material from under the suspect's fingernails; cutting his fingernails; removing material from his nostrils; taking hair samples including root samples; removing material from the surface of the body; skin tests, urine, saliva and air samples; and buccal (cheek) cell samples. The *least invasive test*, defined as a "search over the body of a person," includes those searches that are neither internal nor external and includes the power to search the clothes and personal effects[94] of the individual.

A police officer is empowered to search the surface of the body of a person being arrested. He may conduct an external search if he has reasonable cause to suspect[95] that the suspect's body contains proof of the commission of a felony or misdemeanor or proof of a connection between the suspect and the commission of an offense. If the suspect objects to the search, it may only be conducted with the authorization of a police commander, who is only entitled to authorize a frontal examination of the suspect's body, an examination of the skin, the fingerprinting of certain aspects of the body, removal of material from under the fingernails, and the taking of hair samples and materials from the surface of the body. Internal searches in the body of a suspect may only be authorized by a police commander who has reasonable cause to suspect that the suspect's body contains proof of the commission of a felony (or in the case of a blood test, a misdemeanor) or proof of a connection between the suspect and the commission of an offense as aforesaid. The search may only be conducted after a medical opinion has been given to the effect that there is no medical obstacle to conducting the search and upon obtaining the suspect's consent to the search. If the suspect refuses to consent, a court warrant must be obtained for the search. Any search may be conducted in the body of a person, even if he is not suspected of involvement in an offense, if he provides his consent thereto.

This arrangement provides the police—but not other enforcement agencies—with tools for preempting or investigating crimes generally, although clearly it cannot provide a sufficient answer to the threats posed by terrorism. Consequently, a number of statutory provisions possessing security objectives have expanded and increased the flexibility of the powers they confer. First, in relation to the power to search premises, Regula-

94. The term "effects" means the personal effect then being carried by the individual. *See* Criminal Appeals [Cr. App.] 663/81 Hori v. State of Israel, 36(2) P.D. 85, 90 (Heb.).

95. To establish reasonable cause for suspicion, it is not necessary to collect conclusive evidence that leads to the certain conclusion that the person is involved in the offense. On the other hand, it is not sufficient for the searcher to subjectively believe that there is such involvement without supporting evidence. Reasonable suspicion arises when, after considering all the circumstances (both those which tie and those which free a person from suspicion), a reasonable person would suspect such involvement. *See* H.C. 465/75 Dagni v. Minister of Police, 30(1) P.D. 337 (Heb.).

tion 75 of the Defense (Emergency) Regulations[96] (hereinafter the Regulations) empowers any soldier or police officer to conduct a search in any place—including in vehicles, aircraft, and sea vessels—if he has reasonable cause to suspect that it is being used or will soon be used for a purpose that harms public order or national security or that a person who has committed one of the offenses listed in the Regulations is present therein.

The General Security Service Law[97] (the "GSS Law") grants GSS operatives the right to search the vehicle of a person who crosses Israel's border points, if this is necessary to foil unlawful acts intended to harm national security; to safeguard people, information or places decided upon by the government; to otherwise safeguard or promote national interests essential to the national security of the state. If the GSS operative has reasonable cause to believe that the vehicle contains an item whose seizure is essential to carrying out the operations of the GSS, he is entitled to conduct a search therein even without the presence or knowledge of its owner. Likewise, the law provides that the Prime Minister is entitled to provide written authorization to GSS operatives to search vehicles or premises in the absence and without the knowledge of the occupiers thereof (a "covert search"), if he is persuaded that they contain information vital to carrying out the abovementioned operations of the GSS and that there is no other reasonable method of achieving the purposes of the search. In cases where the search cannot be delayed, the head of the GSS is empowered to authorize the search, but he must notify the Prime Minister thereof within 72 hours of granting such authorization.

The Civil Aviation Law[98] confers discretion upon a security officer, a police officer, a soldier, or a member of the Civil Defense Force ("authorized examiners") to search the vehicle of a person entering the aerodrome or present therein, if the search is necessary in his opinion to ensure public safety.

The Powers of Search (Emergency) Law[99] provides that when a state of emergency exists in the state by virtue of a declaration made under Basic Law: the Government, the authorized examiners may carry out a search of the vehicle of a person upon the entry of that person into any building or enclosed premises, or while present in a sea port, if in their opinion such a search is necessary to protect public security. Likewise, the law enables authorized examiners to carry out a search of vessels upon their entry into a seaport or while present there, if in their opinion such a search is necessary to protect public security. Additionally, power is granted to search vehicles or vessels irrespective of where located, where it is suspected that

96. Defense (Emergency) Regulations 1945, Official Gazette supp. 2 855 (hereinafter the Defense Regulations).

97. Sections 9 and 10 of the General Security Service Law 5762-2002, S.H. 1832, 179 (hereinafter the GSS Law).

98. Section 9 of the Air Navigation (Safety of Civil Aviation) Law, 5757-1977, S.H. 854, 126 (hereinafter the Civil Aviation Law).

99. Section 3 of the Powers of Search (Emergency) (Temporary Provision) Law, 5729-1969, S.H. 571, 226.

there are arms or explosives unlawfully present in such vehicles or vessels as the case may be.

Second, in relation to the power to search the body of suspects, Regulation 76 of the Emergency Regulations vests every soldier or police officer with the power to carry out a search of the body of a person if he has reasonable cause to believe that the person is carrying an article that he used to commit an offense listed in the Regulations, that an offense was committed in relation to it, or that it may be used as evidence of the commission of an offense as aforesaid.

Section 9 of the Civil Aviation Law empowers the authorized examiners to search the body of any person entering or present in any aerodrome or aircraft if in their opinion the search is necessary to protect the security of the public. Where a person refuses to allow his body to be searched, the law categorically prohibits him from being transported and also vests discretion to carry out the search despite the person's refusal, to prevent the person from entering or leaving the aerodrome, or to remove him from the aerodrome.

Section 3 of the Powers of Search (Emergency) (Temporary Provision) Law empowers the authorized examiners to search the body of a person upon entering a building or enclosed premises or while present in a sea port, if in their opinion such a search is necessary to protect public security. Likewise, the law enables authorized examiners to carry out a search of a person's body—irrespective of where he is located—where it is suspected that he is unlawfully carrying arms or explosives.

The Law Regulating Security in Public Bodies[100] requires the bodies listed therein, such as government offices and defense establishment facilities, to appoint a security officer to be responsible for the organization and implementation of its security activities, and it vests that security officer and the guards subordinate to him with the powers of search established by the Powers of Search (Emergency) (Temporary Provision) Law.[101] Section 9 of the GSS Law grants GSS operatives the power to search the body of a person and his personal effects and goods if this is necessary to carry out one of the activities referred to above in relation to the power to search premises (i.e., to foil an unlawful act, to guard public figures, places and information, and to promote interests essential to national security). In the event that the GSS operative has reasonable cause to believe that the effects of a person contain an item whose seizure is essential to carry out the aforesaid activities, he is entitled to search them even in the absence and without the knowledge of their owner.

The above review reveals that the powers of search—both in the premises and on the body of a person—are extremely broad and comprehensive. In the name of state security it is possible to search not only the premises and vehicles of a person suspected of terrorist involvement, but also the

100. Sections 2, 3 and 13 of the Law Regulating Security in Public Bodies, 5758-1998, S.H. 1685, 348.

101. The same also applies to the power to search premises.

premises and vehicles of a person who is not a suspect, sometimes in his absence and without his knowledge. Likewise, it is possible to search the body of a person, even when he is not suspected of involvement in hostile activities.

This brings us, therefore, to the principal question: Is this an appropriate arrangement?

To answer this question we examine two subordinate issues to clarify the precise scope of the above arrangement. First, we shall examine the nature of the technological measures that, when used, comprise a search and focus on the precise significance of the various search powers. Next, we shall examine the criteria used in applying the various search powers. After answering these two questions, we shall be able to draw a conclusion regarding the constitutionality of the search arrangements in Israeli law.

1. *The Technological Measures Which When Used May Be Regarded as Performing a Search*

a. *Searching in a person.* Until the enactment of the Criminal Procedure Law, searches were regulated by Section 22 of the Criminal Procedure Ordinance, which established the power to search the person of the suspect, his clothes, and his effects. The power to search the person of the suspect was interpreted by the case law as limited solely to an external search of the body (following the enactment of the Criminal Procedure Law, this power was divided into a power to conduct an external search and a power to conduct residual searches), in contrast to an internal search of the body, which requires express consent.[102]

Following the amendment of the law, most of the other statutory security provisions were correspondingly amended to clarify that the search powers vested by them are identical to those established by Section 22.[103]

Because the power to conduct an external search embraces a frontal examination of the naked body of the suspect and an examination of the surface of the skin—the two principal procedures required in the circumstances contemplated by Section 22—we may see that in practice it deprives the power to search the surface of a person's body of almost any meaning and leaves the main significance of the latter to searches of the clothing and effects of the suspect.[104]

---

102. Cr. App. 663/81 Hori v. State of Israel, 36(2) P.D. 85, 91-92 (Heb.).

103. The only provision that was not amended was that established in the Defense (Emergency) Regulations. There are those who believe that since reference is to a special search power that is established by defense legislation, it should be interpreted in accordance with the meaning which was accorded to an external search prior to the law being amended and not restricted to the residual power currently set out in Section 22. In my opinion, this interpretation is not only incompatible with the other defense legislation powers but also conflicts with the interpretation required by Basic Law: Human Dignity and Freedom. *See* I. KEDMI, ON CRIMINAL PROCEDURE 392 (vol. A 1992) (Heb.).

104. For this reason there are those who believe that the power to conduct a frontal examination and a skin test should be construed as applying only to activities con-

To date, the case law has not determined which of the investigative methods described above will be deemed to comprise a search, notwithstanding the great importance of clarifying the conditions in which they may be implemented. In view of the definitions assigned to the three categories of search, it is not inconceivable that when these issues are eventually examined, it will be possible to contend that the use of thermal imagers to detect the heat waves emitted by the human body should be regarded as an internal search since they image the interior of the person's body. Likewise, scanning a person's body with radar skin scanners, passive millimeter wave imaging, and x-ray devices should arguably be classed as frontal examinations and therefore external searches.[105] Biometric measures entailing retina and iris identification, fingerprints,[106] palm geometry, and facial and auditory identification should be regarded as taking prints of body parts and therefore as themselves comprising an external search. At the same time, judicial policy reasons may lead to the conclusion that because a person's hand, fingers, features, and voice are bodily characteristics that are generally visible, they should not be regarded as comprising a frontal examination of the *naked* person, but rather as an external search.

b. *Searching premises*: Apart from the physical aspects of the search of a person's premises, the law provides that penetrating computer material also comprises a search, that may only be carried out on the basis of a judicial warrant issued on one of the grounds of search set out in Section 23. Penetrating computer material is defined as: "[p]enetration by means of communicating or connecting with a computer, or by operating it, save for penetration into computer material which comprises tapping under the Secret Monitoring Law, 5739-1979."[107] It follows that the law distinguishes between penetrating a particular computer, which comprises an invasion of the privacy of the computer user and resembles entry into his premises, and monitoring the means of communication between computers. The former case is subject to the laws regulating the search of premises while the latter case is regulated by the Secret Monitoring Law, which shall be discussed below.[108]

2. *Manner of Implementing the Powers of Search–Profiling*

Every day thousands of people pass through the doors of bus stations, shopping centers, tourist sites, sea ports, and airports. Security considera-

---

ducted in relation to intimate parts of the body and that the power of search established by Section 22 should apply to the remaining cases. *See* KEDMI, *supra* note 103, at 378.

105. As these devices image the entire body of a person, this is the law even in the opinion of those who believe that only an examination of intimate parts of the body comprises an external search.

106. This is subject to the limitation set out in Section 13 of the Criminal Procedure Law, to the effect that the restrictions on external searches should not be applied to fingerprints taken solely for identification purposes.

107. Section 4 of the Computers Law, 5755-1995, S.H. 1534, 366.

108. Computer Bill, 5754-1994, Hatzaot Hock 2278, 478.

tions have led the law to permit searches of persons and their effects even though they are not suspected of involvement in any unlawful activities whatsoever. Powers of search in relation to persons who are suspected of terrorist activities are even wider and, inter alia, authorize both internal and external searches of their body. Likewise, security considerations have led the law to permit searches of the vehicle and premises of a person, even though he is not suspected of terrorist involvement.

This explains the importance of the standards that guide the application of these powers.

The search laws are silent on this issue and security considerations preclude the disclosure of the internal directives now in use.[109] In practice, reports issued by human rights organizations[110] and the accounts of journalists[111] show that the powers are operated on a profiling basis, so that those who fit the profile criteria of the potential terrorist are consequently suspected of involvement in terrorist activities and are therefore subject to a prolonged and intensive process of questioning and searches of their bodies, effects and premises, while those who do not conform to the profile are exempt from examination in certain circumstances (for example, where road blocks are set up) or are subject to merely perfunctory

---

109. H.C. 4950/90 Tikvah Franz et al. v. Minister of Defense et al., 47(3) P.D. 36, 43.

110. The press release issued by the Israeli Citizens Rights Association regarding the attitude displayed by "Arkia" Airline security personnel to an Arab passenger is an example:

> Mr. Tlawi wished . . . to travel to Kiryat Shemona on a flight from Sdeh Dov using the Arkia company. However, both during his flight from Sdeh Dov and during his flight back from Kiryat Shemona, Mr. Tlawi was forced to undergo a series of humiliating and insulting interrogations . . . . When the Arkia security personnel in Sdeh Dov became aware that Mr. Tlawi is an Arab he was forced to undergo a series of humiliating and insulting interrogations and checks, whereas other passengers were questioned for a minute or two . . . . Mr. Tlawi was questioned at length both during the flight from Sdeh Dov and during the flight back; his interrogators made it explicit that this was because he is an Arab.

Likewise, see the press release issued by the Israeli Citizens Rights Association regarding the attitude displayed by security personnel in the "Bat Galim" train station in Haifa to an Arab passenger:

> Mr. At'mana is the manager of a youth association which seeks to bring Jewish and Arab youth closer to one another. He was delayed and questioned in an insulting and humiliating manner simply because he is an Arab. There was no reason justifying the different attitude taken to him compared to the other passengers, who at the most underwent a routine baggage check upon entering the train station . . . . Mr. At'mana is not the only Arab citizen who receives different, humiliating and insulting treatment from the security personnel in Israeli train stations. Many Arab citizens of the State of Israel who travel in the trains are forced to undergo an exhausting and insulting series of questions and checks—which far exceed the routine security checks . . . . [T]he circumstances point to the fact that as a whole the Arab citizens of the State of Israel are classified as passengers who pose "a high level" of risk to national security and public safety, as distinct from the other citizens of the state.

These examples are available at http://www.acri.org.il/hebrew-acri/engine/story.asp?id=318; http://www.acri.org.il/hebrew-acri/engine/story.asp?id=237 (last visited July 31, 2003).

111. Rotem, *supra* note 76; A. Segev, *Humiliation Carries a Price*, HA'ARETZ, July 17, 2000.

searches in other circumstances (for example, when passing through sea and airports).

Implementing powers on the basis of profiling entails numerous legal and moral dilemmas. On the moral level, there is an obvious difficulty in determining how to treat an individual based on his affiliation to a particular group because, at least prima facie, perception of him as part of a collective as opposed to as an independent entity worthy of separate consideration, might undermine the most basic tenets of the liberal ideal that forms one of the pillars of the democratic regime. On the legal level, the constitutionality of the use of profiling is not free of doubt, albeit these doubts have not been the subject of judicial attention.

The first doubt concerns the basic question whether as a matter of law it is even possible to exercise the power to conduct a security search in this manner. Administrative law provides that the power must be exercised fairly, equally, reasonably, honestly, and in good faith.[112] The central issue, therefore, is whether profiling is discriminatory and consequently prohibited or, alternatively, whether it is a permitted inquiry.

The principle of equality is a fundamental tenet of Israeli law that has its origin in the Declaration of Independence in which the State of Israel undertook to guarantee the equality of all its citizens without distinction between religion, race, and gender. The principle of equality is not entrenched in Basic Law: Human Dignity and Freedom, but case law has recognized its transformation into a constitutional supralegal right within the framework of human dignity.[113] Equality means the neutral and uniform implementation of normative powers for all individuals save if there is a relevant substantive difference between them, in which case differences in implementation will not amount to unlawful discrimination but will rather be regarded as a lawful distinction.[114]

In my opinion, use of profiling, subject to the restrictions described below, cannot be described as a form of prohibited discrimination. As noted, a profile is composed of a collection of characteristics that are frequently present in known terrorists. When the frequency of a particular characteristic among terrorists (such as nationality, religion, gender, age, family status, or socioeconomic condition) is clearly disproportional relative to its frequency in the rest of the population, it becomes a substantive and weighty issue that justifies and even obligates the state to take extra precautions against those who possess this characteristic, in view of the huge importance of preventing acts of terror.

In the alternative, because equality, like privacy, is a relative value that requires a balance to be drawn when it clashes with the public interest in

112. H.C. 297/82 Berger v. Minister of the Interior, 37(3) P.D. 29, 34 (Heb.).

113. H.C. 721/94 El Al Israel Airlines Ltd. v. Danielovitz, 48(5) P.D. 749, 759-60 (Heb.).

114. A. RUBINSTEIN, THE CONSTITUTIONAL LAW OF THE STATE OF ISRAEL, 285 (5th ed., vol. A 1996) (Heb.).

national security,[115] we may argue that even if profiling *is* discriminatory, the principle of equality will retreat upon the existence of a reasonable likelihood of harm to security.

The second doubt concerns the question whether every characteristic may be used as a profiling criterion or whether those basic characteristics in the democratic experience—race, nationality, and religion—ought to be rejected as legitimate criteria.

Here, too, I believe that the test for regarding *any* characteristic as a relevant and, therefore, legitimate factor is the test of incidence among terrorists. Thus, in circumstances where all the terrorist attacks against the Jewish population in Israel are carried out by Moslem Arabs, failure to take into account the factors of nationality and religion would amount to an irrational and contrived avoidance of reality.[116] At the same time, one cannot disregard the risk of sliding down the slippery slope inherent in dependence on these characteristics,[117] i.e., falling into the trap of creating a stereotypical social climate that legitimizes the racist and degrading treatment of groups in the population, the majority of the members of which abhor the acts of killing no less than the members of groups that are not suspect.

To negate this risk, my view is that profiles based solely on these characteristics should not be permitted; rather, these factors should be integrated into a broader range of characteristics, thereby guaranteeing that not all those affiliated with the particular groups concerned will automatically be subject to such serious violations of their privacy.[118]

The third doubt concerns the efficiency of the profiling system. The theory on which this system is based is that the statistical incidence of particular characteristics possessed by known terrorists is relevant to the identification of potential terrorists.[119] Skeptics argue that because every person follows unique, sometimes strange, practices, it is not possible to identify suspicious patterns of behavior based solely on statistical characteristics.[120] Thus, for example, in the United States, profiling in the air transport sector began at the end of the 1960s, in the aftermath of a wave of airplane hijackings; however, it was stopped in 1972, when it was proved to be ineffective. When profiling was brought back into use in 1998, this time in the shape of the computerized CAPPS version, it only succeeded in identifying two of the aircraft hijackers on September 11, 2001.[121]

While profiling has achieved some success, it has on occasion proved defective both in terms of falsely identifying innocent persons and in failing to identify terrorists. At the same time, no alternative currently availa-

115. H.C. 246/81 Derech Eretz Assoc. v. Broadcasting Authority, 35(4) P.D. 1, 33 (Heb.).

116. Baker, *supra* note 72, at 1398.

117. S.J. Ellmann, *Racial Profiling and Terrorism*, 22 N.Y.L. SCH. J. INT'L & COMP. L. 305, 360 (2003).

118. Braber, *supra* note 74, at 474-75.

119. Baker, *supra* note 72, at 1378.

120. J. STANLEY & B. STEINHARDT, *supra* note 68, at 12.

121. Baker, *supra* note 72, at 1378, 1398.

ble offers a better solution. Avoiding the use of profiling would entail establishing uniform security arrangements for the entire population. Inevitably, to allow people to pursue a normal way of life, the standard of implementation would have to be lower than is currently applied to those who meet the profile criteria. At the same time, the injury caused to the privacy of the entire population would be uniform even though interpretation of the provisions of the search laws in the spirit of the Basic Laws requires that the degree of injury to each individual be compatible with the level of risk posed by each individual.

3. The Constitutionality of the Search Arrangements

The security search powers are scattered through a large number of laws, meaning that drawing a comprehensive picture of the ability of the law enforcement agencies to invade the property and person of individuals in Israel is not an easy task.

We have seen that every person may be subjected to a routine external search of the surface of his body. The search may be conducted by a police officer, soldier, home command officer, or security officer, whereas persons suspected of involvement in terrorism are subject to internal and external searches of their body under the general search power accorded by the Criminal Procedure Law, a power that has been conferred solely on the Israel police force. Likewise, we have seen that use of profiling methods formulates suspicion. It follows that, whereas every person is subject to routine search of the surface of his body, his clothing, and personal effects, only terrorist suspects are subject to more extensive bodily searches.

This principle, while proportional, entails a number of arrangements that infringe the privacy of a person in an excessive manner. *First*, the power to conduct a covert search of the premises and vehicle of a person is not only confined to persons suspected of involvement in terrorist activities, but its exercise is also not subject to prior judicial review (by means of applying to the court for a search warrant, in cases where the search may be delayed) or even retrospective review (in cases where the search is required immediately), and it is sufficient for the Prime Minister to give his approval, or in urgent cases for the head of the GSS to give his approval.[122]

Judicial review in these circumstances is particularly important; whereas the general arrangements relating to the search of premises enable witnesses to be present while the search is carried out to allow them to supervise its performance and prevent overstepping of the search warrant,[123] this right is negated when covert searches are performed. Moreover, the law does not determine whether and when a person whose premises or vehicle is being searched is entitled to know of that search, and consequently that person is deprived of the ability to challenge its validity.

122. Comments of the Israeli Citizens Rights Association regarding the GSS bill, *at* http://www.acri.org.il/hebrew-acri/engine/story.asp?id=372 (last visited Aug. 3, 2003).

123. Section 26 of the Criminal Procedure Law; Misc. App. [Misc. App.] (Jerusalem) 1153/02 State of Israel v. Abergil (as yet unpublished), §§ 26-28 (Heb.).

The power to conduct a covert search of the personal effects and vehicle of a person who crosses a border checkpoint is even more far-reaching, since it does not require authorization of the search, and service personnel may exercise that power at their discretion.

There may indeed be security investigations that will be frustrated if certain persons learn of searches prior to those searches being conducted or while underway; however, it would seem that there can be no justification for allowing such a severe violation of privacy—particularly in cases where the person is not suspected of involvement in an offense—without first applying to a court for a search warrant and thereby guaranteeing its propriety. In cases where there is insufficient time for an application, the search should only be permitted upon authorization by the Prime Minister or the head of the GSS (and this would be appropriate even in relation to covert searches at border checkpoints) subject to an obligation to apply to court for a retroactive warrant affirming the legality of the search.

Likewise, the silence of the law relating to notification should not be interpreted as a negative arrangement exempting the security authorities from the principles of administrative law regarding fairness and reasonableness. Under those principles, notification must be made within a reasonable period of time from the moment the security grounds for secrecy disappear, as it is evident that had the legislature wished to establish an exception in relation to these basic principles, and thereby cause indirect harm to the individual's right to be heard, this would have been done by express legislative provision.[124]

Secondly, when the question of the constitutionality of the border checkpoint lists was made the subject of judicial consideration, the court held that the GSS had to enable those included in the list to challenge the decision in court and, in the event that their application was rejected, to allow them to file an administrative petition to the High Court of Justice against the decision. The court left open the possibility of applying prior judicial review, i.e., establishing a rule whereby a precondition for including a person in the list is that an ex parte application has been made to the court for authorization of this action.[125] The broad language of Section 98 of the GSS Law, which, as noted, permits service personnel to search the body, cargo or vehicle of a person who crosses a border checkpoint, in practice permits use of this list, but without establishing criteria for including or excluding names from the list or, indeed, an alternative mechanism for judicial review.

Because, by its nature, the list is determined in advance, there seems to be no relevant obstacle to the imposition of prior judicial review, except in cases where there are urgent security grounds for swiftly including the name of a person in the list, in which case it is appropriate that the judicial review be conducted retrospectively, as close in time as possible to the time

124. Likud party caucus in Petach Tikvah Municipality v. Council of Petach Tikvah Municipality, 34(2) P.D. 566, 580-81 (Heb.).

125. H.C. 4950/90 Tikvah Franz et al. v. Minister of Defense et al., 47(3) P.D. 36, 43-44.

of its inclusion.[126]

B. Secret Monitoring Within the Framework of Security Investigations

The Secret Monitoring Law[127] regulates the laws applicable to the use of devices for listening in to the conversations of others, without the consent of at least one of the speakers.[128] A "conversation," for the purposes of this law, is defined broadly and includes conversation by word of mouth or by a land line or cordless telephone, communication by way of fax, as well as communications between computers.[129] For our purposes, three types of monitoring are relevant: first, monitoring the conversations of a person within the public domain[130] may only take place upon authorization by the head of a security authority[131] for reasons of national security. Second, monitoring the conversations of a person in private may only be conducted upon written permission given by the Prime Minister or by the Minister of Defense, if they are satisfied that it is necessary to do so for reasons of state security. In cases that require secret monitoring to be carried out without delay and there is no time to obtain a permit, the head of a security authority is empowered to permit such monitoring in writing but must notify the Prime Minister or Minister of Defense of the same forthwith, and the latter may cancel or modify the permit.[132]

The relative ease with which secret monitoring may be carried out in the public domain (compared to that carried out in private) requires that these terms be explained. "Public domain" is defined in Section 8 as "a place where a reasonable person could have expected that his conversations would be monitored without his consent." It follows that the "private domain" is a place where a reasonable person would expect that his conversations would not be monitored. Consequently, the law provides a substantive, objective test: when a person's subjective expectation of privacy (disclosed by his conduct) is reasonable, i.e., is legitimate in the eyes of the public, his conversations must be monitored in accordance with rules applicable to monitoring in the private domain. An expectation of privacy may be reasonable not only in a place where a person has a proprietary interest (such as in his house or vehicle), but also in a public place. Thus, for example, two persons secluding themselves in an isolated spot in a café or a person talking in a public telephone box have legitimate expectations

126. Comments of the Israeli Citizens Rights Association regarding the GSS bill, *supra* note 122.

127. The Secret Monitoring Law, 5739-1979, S.H. 938, 118.

128. Likewise, the law regulates the unusual situation in which a person "talks" to himself.

129. Section 1 of the Secret Monitoring Law defines a conversation as being carried out by "word of mouth or by telecommunications, including by telephone, cordless telephone, mobile radio telephone, wireless communication device, facsimile, telex, teleprinter or communications between computers."

130. Section 8 of the Secret Monitoring Law, *supra* note 127.

131. Section 1 of the law defines a security "authority" as follows: 1. the Intelligence Branch of the General Staff of the Israel Defense Forces; 2. the General Security Service.

132. *Id.* Sections 4 and 5.

of privacy in the eyes of the public, and therefore their communications should be monitored in accordance with the rules applicable to monitoring in the private domain.

The third type refers to monitoring of conversations (in the public or private domain), such as conversations between attorney and client or between doctor and patient, testimony of which is privileged under the Evidence Ordinance.[133] Such monitoring is permitted upon the existence of three cumulative conditions. First, it must be essential for reasons of national security for the purpose of investigating a felony. Second, there must be reasonable cause to suspect that the professional, conversation with whom is privileged, is involved in the offense. Third, upon meeting the two preceding conditions, the President of the District Court has discretion to decide whether or not to grant permission for the monitoring. It should be emphasized that only when this type of monitoring is involved does the law require judicial scrutiny.

There is no dispute that secret monitoring offers great advantages in the investigation of acts of terror, and the fact that the power to monitor is limited solely to the Intelligence Branch of the IDF and to the GSS reduces the potential for harm. At the same time, these facts do not justify the absence of a requirement for judicial scrutiny prior to monitoring being carried out, save in those cases where the urgency of the matter precludes such scrutiny, in which event retroactive judicial scrutiny must suffice.

In addition, while the law requires that a permit to monitor in the private domain include details of the person whose conversations are to be monitored, the mode of monitoring, and the duration of validity of the permit, there is no equivalent provision for monitoring in the public domain, so that at least prima facie, it would seem that the permit may be general in relation to time, mode, location, and the identity of the speakers and the persons authorized to monitor them.[134] When this issue was brought before the court, one opinion was that the existence of restrictions on monitoring in the private domain implied a negative arrangement in relation to the existence of restrictions in the public domain; others thought that rules of proper administration also required the imposition of these rules to monitoring within the public domain.[135]

In my view, an additional defect may be found in the fact that while there is a duty to report annually to the Knesset Committee regarding the number of monitoring permits issued for the private domain, there is no equivalent duty for monitoring in the public domain. This monitoring too violates the privacy of the individual, albeit less severely than monitoring

133. *Id.* Sections 9 and 9A.

134. A. Stein, *Secret Monitoring and Concealed Electronic Surveillance as Means for Promoting Criminal and Security Investigations*, 14 MISHPATIM 527, 544 (1985).

135. Criminal File [Cr. F.] (Tel-Aviv) State of Israel v. Falach, 1981 A District Ct. Judgments 177 (Heb.); Cr. F. (Nazareth) 332/79 State of Israel v. Cohen and others, 1980 B District Ct. Judgments 116 (Heb.); Cr. A. 598/80 Cohen and others v. State of Israel, 35(2) P.D. 393 (Heb.).

in the private domain,n and accordingly it, too, should be subject to public scrutiny in relation to the manner of its implementation.

C. Surveillance, Monitoring, and Photography

The Protection of Privacy Law establishes the rules applicable to about 11 aspects of the right to privacy,[136] three of which are relevant for our purposes: listening in to the conversations of a person without the assistance of technological devices;[137] photographing a person while he is in the private domain, such as installing concealed cameras in the home and vehicle of a person; and spying on, trailing, or other harassment. Clearly the rules on spying on, trailing, or other harassment regulate covert human surveillance of another person;[138] however, one may ask which of the technological measures discussed in Part III also fall within its boundaries. The case law has held that the terms "spying" or "trailing" "refer to external surveillance of the movements of a person,"[139] while the term "other harassment" has been described as "a difficult and unclear expression" that cannot be given a literal definition and accordingly must be interpreted in the light of the statutory purpose that it is intended to achieve.[140] This purpose, in the view of the majority of the judges, confines the scope of its

136. Protection of Privacy Law, 5741-1981, S.H. 1011, 128.
Section 2 of the law provides that infringement of privacy is any of the following:
(1) spying on or trailing a person in a manner likely to harass him, or any other harassment;
(2) listening in prohibited under any law;
(3) photographing a person while he is in the private domain;
(4) publishing a person's photograph under such circumstances that the publication is likely to humiliate him or bring him into contempt;
(5) copying or using, without permission from the addressee or writer, the contents of a letter or any other writing not intended for publication, unless the writing is of historical value or 15 years have passed since the time of writing;
(6) using a person's name, appellation, picture or voice for profit;
(7) infringing a duty of secrecy laid down by law in respect of a person's private affairs;
(8) infringing a duty of secrecy laid down by express or implicit agreement in respect of a person's private affairs;
(9) using or passing on to another, information on a person's private affairs otherwise than for the purpose for which it was given;
(10) publishing or passing on anything obtained by way of an infringement of privacy under paragraphs (1) to (7) or (9); or
(11) publishing any matter relating to a person's intimate life, state of health or conduct in the private domain.
Id.

137. In this connection it is worth noting that in the period between December 2001 and November 2002, Regulation 29(b) of the Prison Regulations, 5738-1978, provided that a meeting between a prisoner and his attorney would take place out of the hearing range of the prison guards, save if there was reasonable cause to suspect that a meeting carried out in this manner would endanger national security. For further elaboration of this issue, see the petition filed by the Association of Civil Rights on this matter, in consequence of which the language of the Regulation was modified, H.C. 1437/02 Association of Civil Rights v. Minister of Internal Security and others, *at* http://www.acri.org.il/hebrew-acri/engine/story.asp?id=385 (last visited Aug. 3, 2003).

138. F.H. 9/83 Military Appeal Court v. Vaknin, 42(3) P.D. 837, 851 (Heb.).

139. H.C. 249/82 Vaknin v. Military Appeal Court, 37(2) P.D. 393, 426 (Heb.).

140. *Id.* at 427-28.

application solely to acts infringing privacy other than by the use of physical force or violence.[141] Consequently, this category would appear to include overt human surveillance, closed circuit camera surveillance in the public domain, use (in public and private) of binoculars, telescope and night vision glasses, and beepers, as well as metal detectors, thermal imagers, passive millimeter wave imaging, radar skin scanners, x-ray cameras and biometric equipment, to the extent that they do not fall within the definition of an external search or a search of the surface of the body.

Whereas the rule is that an infringement of privacy is both a criminal offense and a civil tort, Section 19(b) of the law provides that a security authority[142] or a person acting on its behalf "shall bear no responsibility under this law for an infringement reasonably committed within the scope of its or his functions and for the purpose of carrying them out." From this provision, it follows, first, that an infringement of privacy for security reasons may also be directed against a person who is not suspected of involvement in terrorist activities. The question arises as to the position of an infringement of privacy that requires entry into the premises of an individual to carry it out (for example, installing a surveillance camera in a person's home or planting a beeper in his property). Section 17(b) of the Interpretation Law[143] grants a person who has been affirmatively empowered to do something the auxiliary powers reasonably required to perform that function; however, the Protection of Privacy Law does not grant the security authorities an affirmative power but merely an exemption[144] Accordingly, to carry out these powers it would seem necessary to obtain a warrant permitting entry into the premises of the individual. Second, the test of the reasonableness of the infringement, which is a precondition for a discharge from liability, is amorphous and lacks any real meaning, and indeed to date the courts have refrained from establishing standards for its application. It seems to me that the reasonableness of the infringement of privacy should be established in the light of all the circumstances of the specific case, with special emphasis placed on the manner and severity of the infringement.

As noted, the law is applicable to many of the devices for infringing privacy described in Part III. At the same time, these devices differ from each other, not only in the gravity of the infringement of privacy but also in their level of efficiency. Thus, for example, we have considered the relative degrees of reliability of the range of biometric devices. Studies conducted in the United States and Britain have raised doubts as to the efficiency of closed circuit television cameras in preventing crime, including acts of terrorism. The monotony involved in watching the television

141. F.H. 9/83 Military Appeal Court v. Vaknin, 42(3) P.D. 837, 851 (Heb.).

142. The definition of a security authority for the purpose of this law is broader than that provided in the Secret Monitoring Law and includes the Israel Police, the Intelligence Branch of the General Staff and the Military Police of the Israel Defense Forces, the General Security Service, and the Intelligence and Special Duties Branch, see Section 19(c) of the Protection of Privacy Law, *supra* note 136.

143. The Interpretation Law, 5741-1981, S.H. 1030, 302.

144. Stein, *supra* note 134, at 555.

screens leads to a decrease in concentration of the personnel manning the control centers to below average levels after only twenty minutes of watching, and therefore the likelihood of identifying suspect movements is extremely low.[145] Consequently, the greater the harm caused by a device to the privacy of an individual, and the darker the shadow hovering over the compatibility of the device with the purpose of the investigation, the more stringent should be the conditions for applying the defense of reasonableness.

Third, as the law does not grant affirmative powers to perform acts that infringe privacy, but merely a retroactive discharge from liability, there is no requirement for judicial review or accountability towards any body—prior to or subsequent to the infringement. Review, so it seems, will only take place in those cases where the subject appeals against the legality of the injury. This process is largely a fiction because many of the infringements of privacy take place without the knowledge of the injured individual and consequently he is not aware of the possibility of appealing against it. These problems are particularly serious in view of the doubtful efficiency of many of these infringing devices.

Accordingly, I believe that it would be right to set qualifications on the protection accorded to the above all-encompassing exemption, so that it will only apply upon the existence of the following conditions:

1. Since the exemption cannot be regarded as an affirmative authorization to infringe privacy, it is not possible to compel the security authority to apply to the court in advance for a judicial warrant permitting the infringement, but it is possible merely to compel it to apply to the court shortly *after* commission of the infringement (or in the event of a continuing infringement—shortly after the commencement of the infringement).[146]

2. It is necessary to establish a duty to make an accounting at regular intervals, including details of the number, nature, objectives, and results of the infringements committed during the period of time being reported.

3. As stated in relation to the power to conduct covert searches, here too it is necessary to apply the rule whereby the subject of the search is notified of the infringement, after the security grounds justifying absence of notification have ceased to exist.

D. Data Bases

The Protection of Privacy Law regulates the law applicable to data bases and provides that every data base must be registered in a Register of Data Bases, if one of the following situations applies:

1. The number of people in respect of whom there is information in the data base exceeds 10,000;

2. The data base contains sensitive information;

145. J. STANLEY & B. STEINHARDT, *supra* note 68, at 3.
146. Stein, *supra* note 134, at 556.

3. The data base contains information on people and the information was not provided to this data base by them, or on their behalf or with their consent;

4. The data base belongs to a public entity within the meaning of Section 23;

5. The data base is used for direct mailing as provided in Section 17C.[147]

Whereas the rule entitles a person to peruse information about himself that is held in a data base, Section 13(e) negates the application of this right to a data base controlled by a security authority. Additionally, the Registrar of Data Bases manages a Register of Data Bases, which is open to public inspection (the Register contains details of the identity of the owner of the data base, the purpose for establishing it, the types of information contained therein, and the like). Section 12 provides that for data bases of a security authority, only the identity of the owner of the data base and the purpose for establishing it are open to public inspection. An additional qualification set out in the law provides that whereas a public body is prohibited from divulging information regarding a person, Section 23B provides that the security authorities are not subject to this limitation and may receive or transmit information, provided that the receipt or transmission of information is required to fulfill their functions and is not prohibited by law.

E. Other Infringements of Privacy:

1. Opening Post

Regulation 89 of the Defense Regulations grants the Post Censor power to order the opening of any post that he believes may harm national security or public safety. Regulation 90 grants postal office personnel who have been so authorized by the Director of the Post Office the power to demand that a sender of post present its contents for inspection as a condition for sending it through the post office.

2. Entering Premises Without Search

I. Section 6 of the Civil Aviation Law empowers the Minister of Transport to order measures to be taken to safeguard the aviation facility in the land adjacent to the facility, allowing those carrying out the measures to enter the land, set up equipment, and enclose it. These measures do not require the consent of the occupier of the land or judicial scrutiny, and a person who believes that he has been injured by these orders is entitled to apply to an appeals committee.

II. The GSS Law empowers GSS operatives to enter premises that are not closed private buildings to carry out activities necessary to protect persons, places or information within the responsibility of the GSS. Entry for up to 12 hours does not necessitate the consent of the occupier of the premises nor authorization by a court. Entry for a longer period of time

147. Section 8(c) of the Protection of Privacy Law, *supra* note 136.

requires the consent of the occupier, and in its absence authorization by the court.

In my opinion, it is highly doubtful whether the infringement permitted by these two provisions is proportional. Section 7 of the Basic Law prohibits entry into the private domain of an individual without his consent whether the private domain is closed (for example, a house) or whether it is open (for example, a yard). An all-embracing power to enter open premises without the consent of the occupier and without judicial scrutiny for up to 12 hours (in the GSS Law), and a fortiori without limitation of time (in the Civil Aviation Law), is not proportional because in the vast majority of cases, entry into premises is planned in advance and there is ample time to apply to the court for a warrant.[148] Consequently, it would be appropriate to modify these provisions and provide that every entry into premises requires the consent of the occupier and, in the alternative, a judicial warrant, save in urgent circumstances where it is necessary to effect immediate entry into the premises and time does not permit an application to the court for a warrant (in which case entry into the premises should be permitted subject to an obligation to apply to the court for a permit to remain in the premises).

3. *Receipt of Communication Data*

Section 11 of the GSS Law enables the head of the GSS to demand statutory communication license holders (such as telephone and cable companies) to transmit to the GSS information[149] located in data banks under their control, if this is necessary to fulfill the functions of the GSS. The law requires the head of the GSS to report periodically to the Prime Minister, the Attorney General, and the Knesset Committee overseeing the GSS. The application of the section depends on the establishment of regulations regarding the types of information and the details of the report; these regulations have not yet been promulgated. Likewise, Section 13 of the Telecommunications Law[150] requires the licensee, upon being given an order by the Minister of Communication, to provide telecommunication services to the security services,[151] if considerations of national security or public safety so require. Thus, for example, the Minister may require the cellular telephone companies to install broadcasting antennas in certain areas to allow the movements of their subscribers to be tracked.

Over many years, the State of Israel shaped its array of constitutional balances between national security and individual rights, including the right to privacy, under the shadow of continuous security threats. Accord-

148. *See* comments of the Israeli Citizens Rights Association regarding the GSS bill, *supra* note 122.

149. Information for the purpose of this section does not apply to the *content* of a conversation within the meaning of the Secret Monitoring Law, in contrast to identifying details concerning the conversation.

150. Telecommunications Law, 5742-1982, S.H. 1060, 218.

151. For this purpose, "security forces" are defined as the Israel Defense Forces, the Israel Police, the General Security Service, and the Intelligence and Special Duties Branch. *See* Section 13(a) of the Telecommunications Law, *id.*

ingly, it is not surprising that, while the events of September 11th led many democratic countries to carry out far reaching changes to their traditional array of balances,[152] in Israel no real constitutional changes were undertaken. Nonetheless, as we have seen, this fact alone is not evidence of the appropriateness of the balances currently in place.

From the procedural point of view, the fact that current regulations are spread over a large number of statutes makes it difficult to draw an overall picture of the powers that infringe privacy on grounds of national security. The substantive danger arising from this eclectic arrangement lies in the need to examine the need for each of the powers from the micro perspective of the statute within the framework of which the specific power is granted (one tree in a wood) instead of from the macro perspective of the entire body of powers granted by the various laws (the wood as a whole). The outcome is the grant of gratuitous powers that infringe privacy to an unnecessary extent.

An examination of the prevailing situation reveals that in many cases this has indeed occurred. In addition to the conferral of gratuitous powers, the laws occasionally permit the infringement of privacy without establishing mechanisms for prior judicial review or even retroactive oversight mechanisms and also fail to prescribe arrangements for notifying the individual of the infringement of his rights.

An additional issue that must be considered in this context concerns the lack of transparency regarding the manner of exercising the powers. The Freedom of Information Law expressly prohibits a public authority from transmitting information to a citizen or to a resident of the state that may cause harm to national security or to the safety of the public.[153] Democracies, so it is said, die behind closed doors,[154] because unrestrained power tends to corrupt.[155] The absence of transparency makes it more difficult both for the individual who has been harmed and for the human rights organizations to bring these weighty issues before the courts; consequently, despite the importance and critical character of these provisions, they should not be interpreted over broadly.

I shall now turn to a discussion of the balances between the right to privacy and national security established by a number of other democratic states.

IV. A Comparative View

A. The United States

The right of a person to legal protection from having his privacy interfered with by the law enforcement agencies is not expressly entrenched in the constitutional documents of the United States, i.e., the Constitution

152. A broad comparative review of this issue is set out in the next section.

153. Section 9(a) of the Freedom of Information Law, 1998, S.H. 1667, 226.

154. Detroit Free Press et al. v. Ashcroft et al., 195 F. Supp 2d 937 (E.D. Mich. 2002).

155. I. Osterdahl, *Openness v. Secrecy: Public Access to Documents in Sweden and the European Union*, 23(4) E. L. Rev. 336 (1998).

and the Bill of Rights.[156] Nonetheless, over the years the Federal Supreme Court has interpreted the Amendments to the Constitution, and chiefly the Fourth Amendment, as granting express or implied constitutional protection to certain aspects of privacy.[157]

Even though, prima facie, the Constitution establishes absolute human rights, the fact that it does not refer to conditions for infringing those rights has led the courts to recognize that they may be limited upon the existence of critical public interests.[158]

This section will open with a brief historical review of the activist interpretation given by the Supreme Court to the Fourth Amendment to the Constitution and to the ramifications this interpretation has for the scope of the protection accorded to the right to privacy. This will be followed by an examination of the array of balances between national security and privacy that prevailed on the eve of the terrorist attacks of September 2001, and I shall conclude by examining how the legal response offered by the United States to these attacks has influenced this array of balances.

The Fourth Amendment to the Constitution provides as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[159]

Unlike the legal situation in Israel, American law does not define the term "search" in the Fourth Amendment. Until *Katz v. United States* in 1967,[160] the courts interpreted this term in the light of the trespass doctrine, so that a search was conducted whenever a person's property rights in his body or concrete assets were violated.[161]

The more sophisticated the developments in electronic surveillance technology became, the less this doctrine proved adequate to grant the individual proper protection against the state's invasion of his private life.[162] Thus, for example, monitoring the conversations of a person by means which did not require physical entry into his premises was not regarded as a search and therefore was not subject to the restrictions of the Fourth Amendment. To remain loyal to the rationale underlying the Fourth Amendment, the court adapted its interpretation to the changing times and in the Katz case abolished the trespass doctrine and replaced it with the reasonable expectation of privacy doctrine. Holding that "the Fourth

156. D.H. Flaherty, *On the Utility of Constitutional Rights to Privacy and Data Protection*, 41 CASE W. L. REV. 831, 837 (1991).

157. Griswold v. Connecticut, 381 U.S. 479, 482 (1965).

158. L. Henkin, *Privacy and Autonomy*, 74 COLUM. L. REV. 1410, 1420 (1974); Barak, *supra* note 79, at 522.

159. U.S. CONST. amend. IV.

160. Katz v. United States, 389 U.S. 347 (1967).

161. Olmstead v. United States, 277 U.S. 438, 464 (1928).

162. Berger v. New York, 388 U.S. 41, 49 (1967).

Amendment protects people not places,"[163] the court stated that "search" means infringement of a person's protected interest in the privacy of his life:

> What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[164]

In an opinion, which later case law adopted as the guiding principle of law, Justice Harlan interpreted this principle as comprising two cumulative conditions:

> First that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as "reasonable."[165]

In view of this ruling, it has been held that a person's subjective expectation that no one will search the contents of garbage he has discarded in a public place outside his home is not reasonable.[166] Likewise, the expectation that air surveillance of movements in the private domain will not be carried out is not reasonable, at least so long as the tracker is not assisted by sophisticated technological aids or observes intimate activities.[167] Similarly, tracking the location of a person with a beeper is not a search, so long as the article in which the device has been placed is located in the public domain so that the person's movements can be tracked without technological assistance. Consequently, when the article is placed within a private home, continued tracking will be deemed to be a search.[168] Similarly, use of a thermal imager to detect the amount of heat emitted from the house of a person is regarded as a search, as the information acquired by the tracker in relation to what is happening within the house could only have been acquired by physical entry into its boundaries.[169] Regarding the use of biometric measures, the Court has held that "[f]ingerprinting involves none of the probing into an individual's private life and thoughts that marks an interrogation or search."[170]

The Court also held as follows:

> The physical characteristics of a person's voice, its tone and manner, as opposed to the content of a specific conversation, are constantly exposed to the public. Like a man's facial characteristics, or handwriting, his voice is repeatedly produced for others to hear. No person can have a reasonable expectation that others will not know the sound of his voice, any more than

163. *Katz*, 389 U.S. at 351.
164. *Id.*
165. *Id.* at 361.
166. California v. Greenwood, 486 U.S. 35 (1988).
167. Dow Chemicals Co. v. United States, 476 U.S. 227, 238 (1986); *see* FISHMAN & MCKENNA, *supra* note 41, at 29:11, 29-23.
168. United States v. Karo, 468 U.S. 705, 715 (1984); *see* United States v. Knotts, 460 U.S. 276, 285 (1983).
169. Kyllo v. United States, 533 U.S. 27 (2001).
170. Davis v. Mississippi, 394 U.S. 721, 727 (1969).

he can reasonably expect that his face will be a mystery to the world.[171]

It follows from this reasoning that means of identification using voice, signature, features, palm print, and fingerprints are not in the nature of a search. However, in *Skinner v. Railway Labor Executives' Association*,[172] the Court held that activities that entail entry into the body of a person (such as a blood test) and activities that lead to the disclosure of medical information about a person are activities that violate the individual's reasonable expectation of privacy and consequently comprise a search. In view of this reasoning, which was subsequent to that described above, all biometric measures—including identification by means of voice, signature, features, palm print, and fingerprints—that meet at least one of the two criteria, are in the nature of a search.

Once it is decided that a particular act comprises a search, it must satisfy the conditions of the Fourth Amendment to be regarded as constitutional, i.e., it must be reasonable and carried out under a judicial warrant that clearly defines the article that is being sought. The person applying for the search warrant must have sworn an affidavit showing probable cause for the involvement of the person who is the subject of the warrant in an offense that has been committed or that is about to be committed.

However, over the years, the case law has established a number of exceptions to the requirement for a warrant. The relevant exceptions for our purposes are as follows:

A. Stop and frisk search: Law enforcement agencies are empowered to detain any person who gives rise to a reasonable suspicion that he is involved in criminal activities. During the course of the detention, the law enforcement agent is entitled to search the person's clothes if he has reasonable cause to believe that the latter is armed and therefore poses a danger to him or to the public.[173]

B. Administrative search: As the application of the previous doctrine is limited to situations where there is reasonable cause to suspect that a person is dangerous, it does not provide an answer to situations where locating weapons and explosives requires routine searches to be carried out; for example, searches of the person and baggage of all the passengers in a plane or visitors to a tourist site. To enable preventive searches to be carried out, the case law has developed the doctrine of the administrative search, which has been defined as a search that is conducted "as part of a general regulatory scheme in furtherance of an administrative purpose, rather than as part of a criminal investigation to secure evidence of crime . . . ."[174]

Consequently, for a search to be regarded as administrative, the reason for it must be compelling. This is undoubtedly the case for security

171. United States v. Dionisio, 410 U.S. 1, 14 (1973).

172. Skinner v. Ry. Labor Executives' Assoc., 489 U.S. 602 (1989).

173. Terry v. Ohio, 392 U.S. 1 (1968); United States v. Bell, 464 F.2d 667, 673 (2d Cir. 1972).

174. United States v. Davis, 482 F.2d 893, 908 (9th Cir. 1973).

searches aimed at uncovering weapons and explosives; the search must be confined to achieving this purpose and it must be conducted following the exercise of discretion based solely on relevant considerations.[175]

Even after establishing this doctrine, the courts remained cognizant of the severe injury caused to the privacy of innocent persons:

> The intrusion into our privacy—and an intrusion it surely is—is accepted by most travellers with equanimity . . . . The unavoidable consequence of this exhaustive search for weapons is that security personnel will become aware of many personal items that do not pose a danger to air safety. X-rays reveal, in outline, the contents of packages, often giving a good indication as to their inventory. When packages are opened, or when pockets are emptied, FTS agents will see many items that are considered private.[176]

However, in view of the huge devastation—both to people and to property—that terrorist attacks may potentially cause, it has been held that the benefits arising from conducting the search outweigh the inherent damage entailed by the search, and accordingly it satisfies the constitutional test of reasonableness.[177]

C. Search by consent: The free and voluntary consent by a person to have his body or personal effects searched negates the need for a warrant. Thus, it may be said that a person who is aware that a search may be conducted of his body or possessions in certain situations, such as prior to boarding an airplane, and who freely puts himself in that situation, thereby communicates his implied consent to the search.[178]

In cases requiring a search warrant, the Fourth Amendment provides that the court must issue it if the requirements of reasonableness and probable cause are satisfied. In this context, the Court has held first that "[w]hether a particular search meets the reasonableness standard is judged by balancing its intrusion on the individual's Fourth Amendment interests against its promotion of legitimate government interests."[179]

Secondly:

> "Probable cause" is the standard by which a particular decision to search is tested against the constitutional mandate of reasonableness . . . . In determining whether a particular inspection is reasonable—and thus in determining whether there is probable cause to issue a warrant for that inspection—the need for the inspection must be weighed in terms of these reasonable goals of code enforcement.[180]

Relying on these pronouncements, it may be stated that in times of emergency, when the state finds itself under terrorist attack or facing a real threat of attack, it is possible to lower the standards for examining the

---

175. *Id.* at 910; Camara v. Municipal Court, 387 U.S. 523, 532, 536 (1967).

176. United States v. $124,570 United States Currency, 873 F.2d 1240, 1242-43 (9th Cir. 1989).

177. *Davis*, 482 F.2d at 910.

178. Schneckloth v. Bustamonte, 412 U.S. 218, 248-49 (1973); Unites States v. Miner, 484 F.2d 1075 (9th Cir. 1973).

179. Veronica School District 47J v. Acton, 515 U.S. 646, 652-53 (1995).

180. *Camara*, 387 U.S. at 534-35 (1967).

existence of probable cause below the level of proof needed to obtain a search warrant for ordinary criminal offenses. However, care must be taken not to lower the standard of proof so excessively as to deprive of meaning the requirement of proof of probable cause.[181]

Against this backdrop, I shall now turn to an examination of the federal antiterrorism legislation prevailing prior to the attack of September 11, 2001.

Title III of the Omnibus Crime Control and Safe Street Act[182] and the Electronic Communications Privacy Act[183] (ECPA) regulate the law applying to the monitoring of verbal communications and the monitoring of electronic and wire communications. Monitoring depends upon a judicial warrant, which may only be granted if the monitoring is sought within the framework of a criminal investigation of an offense listed in the law, and if the applicant has satisfied the stringent standard of proof, which requires the following:

> probable cause for belief that an individual is committing, has committed, or is about to commit a particular offence . . . probable cause for belief that particular communications concerning that offence will be obtained through such interception . . . [and] normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous.[184]

Monitoring by means of pen register and trap and trace devices is conducted by virtue of judicial warrants issued under the Foreign Intelligence Surveillance Act (FISA)[185] or the Pen/Trap Statute.[186] Probable cause need not be shown to obtain a warrant; rather, it must be proved that the information that will be seized is relevant to a criminal investigation or to an investigation of international terrorism or foreign intelligence. Apart from engaging in pen/trap monitoring within the framework of investigations aimed at defending national security or gathering foreign intelligence, FISA controls the legal regime applicable to electronic tapping, physical entry into premises, and obtaining records—when these activities are required for investigating the issues mentioned above. Unlike the stringent standard Title III requires to obtain a judicial warrant, FISA requires a lower standard; save if the suspect is a citizen of the United States, in which case probable cause is required of his involvement in activities contravening the criminal law.

The Anti-Terrorism and Effective Death Penalty Act[187] was enacted in the aftermath of the first terrorist attack on the Twin Towers in 1993 and

181. E. Gross, *The Influence of Terrorist Attacks on Human Rights in the United States: The Aftermath of September 11, 2001*, 28 N.C. J. INT'L L. & COM. REG. 1, 31 (2002).
182. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § 2510 (1968).
183. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).
184. Omnibus Crime Control and Safe Streets Act of 1968 § 2518.
185. Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 (2000).
186. 18 U.S.C. § 3121 (2000).
187. Pub. L. No. 104-132, 110 Stat. § 1214 (1996).

the terrorist attack on the federal offices building in Oklahoma City in 1995. Among its provisions, Section 804 allows governmental bodies to compel communication providers to preserve their records regarding customers who are suspected of having committed offenses, for an initial period of ninety days, subject to an option to extend the period for an additional identical period.

Section 303 requires every financial institution that knows it possesses monies associated with a foreign terrorist organization to continue to hold those funds and concurrently report their existence to the authorities. Section 701 removes from the application of Title III information stored in communication systems used for storing and transferring monies, thereby lessening the standard of proof that authorities must meet when seeking information about bank accounts.

On September 11, 2001, the American people experienced one of the most shocking and brutal events in their history. Perhaps it was the sight of the passenger planes crashing, one after the other, into one of the best-known symbols of America; perhaps it was the huge frustration generated by the inability to save the thousands of people caught up in this disaster, whose lives were ended in an act of indescribable cruelty; or perhaps it was the sight of the collapse, destruction, and ruin, but it seemed that the nation as a whole was swept by a sense of cultural and social change—individualism compacted in favor of the general welfare, and individuals displayed a greater willingness than before to sacrifice their freedoms in favor of national interests.

The American government hastened to initiate legislation that reflected this change—not only in its title—"Patriot Act"[188]—but also in the unequivocal tilting of the constitutional balance in favor of national security needs at the expense of individual rights.

Even though the purpose of the law is to strengthen the ability of the law enforcement agencies to fight terrorism, many of the statutory provisions may be used in ordinary criminal investigations. Likewise, in a number of situations, the statutory provisions negate the court's discretion and turn it into a rubber stamp engaging purely in symbolic judicial review. The examples of this are many and I shall confine myself here to those touching upon the right to privacy.

Prior to the enactment of the law, the rules of criminal procedure and the judgments of the state courts interpreted the Fourth Amendment as compelling the law enforcement agencies to notify a person of a search that was about to be carried out in his premises (knock and announce principle), save where certain exceptions applied that varied from state to state and that allowed covert searches to be carried out subject to retroactive

188. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272.

notification.[189] As a result of claims by the law enforcement agencies that the variations in the laws of the various states undermined interstate investigations, including investigations of terrorism, the Patriot Act established a uniform federal standard. Under this standard, in criminal investigations, the court is empowered to authorize a search without prior notice being given, upon reasonable proof that notice would have a deleterious effect on the investigation (for example, it might endanger the life or well-being of a person, allow a person to abscond, interfere with evidence, or frighten witnesses).[190]

Prior to this law, the FISA granted the FBI power to apply to the court for an order compelling a closed list of bodies to hand over records in their possession regarding a person in respect of whom there were "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[191]

The Patriot Act significantly expands this power by enabling the FBI to demand not only records but also "any tangible things," not only from the closed list of bodies but from any body or person (such as a book shop or internet service provider), and not only in cases where there is reason to believe that the subject of the information request is a foreign agent, but where any person is involved. The judicial supervision of the exercise of the power is a pretense because once the FBI has informed the court that it needs the information for the purpose of an authorized investigation relating to international terrorism or secret foreign intelligence, the judge has no discretion to refuse. Moreover, the body or person obliged to hand over the information is prohibited from telling this to anyone else, even in cases where there is no security justification for secrecy, and consequently the person whose privacy has been infringed will never know of it and naturally will not be able to challenge the legality of the search.[192]

As we have seen, even before the Patriot Act, the obstacle to obtaining a judicial pen/trap order was overcome relatively easily. Section 216 of the Act expands this power even further in three respects:[193] first, whereas in the past the validity of the warrant was limited to the area of jurisdiction of the court that issued the order, now courts are entitled to issue warrants valid throughout the United States, and there is also no requirement to identify the article that is the subject of the search. Second, the Act clarifies that it is possible to monitor not only telephone communication networks but also a range of other communication technologies—a pre-Act contentious issue.[194] Third, the Act expands the types of pen/trap information that may be made the subject of the order; however, because it does not contain an explicit definition distinguishing between content and pen/

189. *See* the guidelines of the Department of Justice regarding implementation of the powers under the law, *at* http://www.epic.org/privacy/terrorism/DOJ_guidance.pdf (last visited Aug. 6, 2003).

190. USA PATRIOT Act § 213 (amending 18 U.S.C. § 3103a).

191. 50 U.S.C. § 1862.

192. USA PATRIOT Act § 215 (amending 50 U.S.C. § 1816).

193. USA PATRIOT Act § 216 (amending 18 U.S.C. § 3121(c)).

194. Guidelines of the Department of Justice, *supra* note 189.

trap information, there is room here for an expansive interpretation. Thus, for example, there is a dispute whether the addresses of internet sites should be seen as purely technical information or as information relating to content, as they have the potential to disclose personal information about the areas of interest of the user.[195]

Section 214 of the Act expands the situations in which a pen/trap warrant will be granted under FISA, stating that an order may be sought in "any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[196]

Sections 201 and 202 broaden the application of Title III to investigations of terror offenses, offenses relating to the manufacture and distribution of chemical weapons and computer offenses, and thereby allow a wiretapping order to be granted in respect of them.[197] Because FISA in any event grants broad powers to monitor persons suspected of involvement in international terrorism, it follows that the dominant purpose of the amendment is to enable the monitoring of a United States citizen and domestic terrorist suspects.[198] In addition to the far ranging surveillance powers available under Title III and FISA, as of October 31, 2001, regulations have come into force that enable conversations between a prisoner and his attorney to be monitored without a court order in cases where there is a suspicion that the prisoner will try to transfer information endangering national security through his attorney. However, it should be noted that the regulations require that notification of monitoring be given to the attorney and his client.[199]

In the past, when a criminal investigation was underway, the law enforcement agencies could issue an administrative subpoena compelling suppliers of electronic communication services to hand over limited information regarding their subscribers (such as their name, address, and telephone account). Section 210 of the Act expands the type of information that may be sought under the subpoena to include, inter alia, information regarding the subscriber's means of payment (such as the credit card number or bank account number) and records of the dates and hours of surfing on the internet.

In the past it was possible to apply under FISA for a warrant for electronic surveillance and search of premises for investigations that had the *sole* purpose of gathering foreign intelligence. Section 218 expands the application of FISA to investigations where intelligence gathering is a *significant purpose* but not the sole purpose. As the ground for application is

195. AMERICAN CIVIL LIBERTIES UNION, SURVEILLANCE UNDER THE USA PATRIOT ACT, *at* http://www.aclu.org/SafeandFree.cfm?ID=12263c=206 (last visited Aug. 5, 2003).

196. USA PATRIOT Act § 214 (amending 50 U.S.C. § 1842).

197. USA PATRIOT Act §§ 201, 202 (amending 18 U.S.C. §§ 2516(1), 2516(1)(C)).

198. The broad definition of "domestic terrorism" given in § 802 gives rise to the danger that this power will be exploited against legitimate political opponents of the regime. Gross, *supra* note 181, at 6.

199. National Security; Prevention of Acts of Violence and Terrorism, 66 Fed. Reg. 55,062 (Oct. 31, 2001).

vague, there is a danger that it will be construed broadly so that the easier statutory standard will also be used for criminal investigations.

Section 203 enables the federal law enforcement agencies to exchange information regarding foreign intelligence, originating from wiretapping, without judicial oversight and without requiring the information to be connected to the investigation where wiretapping was allowed. Likewise, the section enables the authorities to receive information in the possession of a grand jury that relates to foreign intelligence.

Section 206 enables a roving wiretap order to be granted, under FISA, to every communications medium used by the subject of the surveillance, if it is proved that he regularly changes his means of communication and thereby thwarts the investigation. The Act does not require the authority to ensure that the subject is indeed using the particular means of communication prior to conducting the wiretap, and therefore the danger arises that innocent people will be monitored.

Section 209 removes the monitoring of vocal mail messages from the application of Title III and also lowers the standard that must be satisfied to monitor them.

Section 212 enables electronic communication providers to voluntarily divulge to the law enforcement agencies records relating to their subscribers in emergency cases involving immediate danger of death or serious physical injury to any person.

Section 217 enables victims of computer attacks to ask the authorities to locate the attacker, and for this purpose the authorities are empowered to monitor activities of the owner of the trespassing computer without a search warrant.

Section 351 permits any financial institution to voluntarily divulge to the authorities information relating to financial transactions that are suspected of violating U.S. laws, without bearing liability for breach of confidence.

It should be pointed out that despite the significant expansion of its powers the government remains of the opinion that it is insufficiently equipped to wage its war against terror. Accordingly, it is now seeking to augment its powers by enacting the Domestic Enhancement Security Act. This Act would infringe the right to privacy—as well as other fundamental rights—even more severely than its predecessor.[200] Thus, inter alia, Section 101 expands the application of FISA by amending the definition of people included in the term "foreign power." Section 102 would enable the monitoring of any person who is suspected of engaging in clandestine intelligence gathering activities for a foreign power, even if his activities are not unlawful. Section 103 provides that electronic surveillance, physical searches, or pen registers may be used for a period of 15 days following a congressional declaration of war or terrorist attack without obtaining a

200. Comments of the American Civil Liberties Union regarding the bill, *at* http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=11835&rc=206 (last visited August 5, 2003).

search order. Section 126 enables the government to obtain the credit records of any person without a search warrant. Sections 128 and 129 enable the authorities to issue administrative subpoenas when a terrorist investigation is underway, requiring any person or body to divulge information in his possession without need for a court order.

B. Canada

The Canadian Charter of Rights and Freedoms,[201] like the constitutional documents of the United States, does not expressly entrench the right to privacy. Accordingly, the Canadian courts have followed the example of their American colleagues and have interpreted Section 8 of the Charter[202]—which confers protection upon the individual against unreasonable searches—as impliedly entrenching the individual's reasonable expectation of privacy.[203]

The restriction of rights set out in the Charter, like the restriction of rights established by Basic Law: Human Dignity and Freedom, is only constitutional if it satisfies the requirements of the limitation clause set out in Section 1.[204] First, it must be made by virtue of law. Second, it must be the type of restriction that may be justified in the light of the values of a free and democratic society, i.e., the purpose of the limitation must be to serve essential social needs—"concerns that are pressing and substantial."[205] Third, it must be reasonable, i.e., the proper purpose must be achieved by selecting the means that cause the least harm to the protected right or freedom.[206]

The two principal federal statutes protecting privacy are the Privacy Act[207] and the Personal Information Protection and Electronic Documents Act (PIPEDA).[208]

The Privacy Act regulates the modes of gathering, use, and disclosure of personal information in the hands of the federal authorities. Section 4 provides that the authorities are empowered to gather information regarding individuals to the extent that it relates directly to an operating program or activity of the institution. Section 8 prohibits the disclosure of this information, without the consent of the individual to whom it relates, save in a number of exceptional cases, including disclosure following a request by a law enforcement agency that needs the information for its investigations

201. Charter of Rights and Freedoms Constitution Act, 1982.

202. *Id.* Section 8 of the Charter provides as follows: "Everyone has the right to be secure against unreasonable search or seizure."

203. Hunter et al. v. Southam Inc., 2 S.C.R. 145, 159 (1984).

204. Charter of Rights and Freedoms Constitution Act, 1982. Section 1 of the Charter provides as follows: "The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society."

205. R. v. Oakes, 1 S.C.R. 103, 138 (1986).

206. *Id.*

207. Privacy Act, R.S. 1985, c. P-21.

208. Bill C-6, Personal Information Protection and Electronic Documents Act, Assented to Apr. 13, 2000.

and disclosure in cases where the public interest in disclosure outweighs the damage that may be caused to the individual by the invasion of his privacy.

Section 12 grants every individual who is a Canadian citizen or a permanent resident access to any personal information relating to that individual under the control of a government institution, subject to a number of exceptions. Thus, for example, Section 22 provides that the authority is entitled to refuse to disclose any personal information requested that was obtained by any investigative government institution during a criminal investigation, pertaining to the enforcement of any law of Canada or an investigation pertaining to activities suspected of constituting threats to the security of Canada. Another exception to the right of access is set out in Section 25, which enables an institution to refuse a request where disclosure could reasonably be expected to threaten the safety of individuals.

PIPEFA establishes the law applicable to personal information held by private commercial bodies whose activities are regulated by federal laws (such as communication companies, banks, and airline companies).[209] Inter alia, Section 7(3) enables those companies to disclose information in their control, without the knowledge or consent of the person to whom it relates, if the information has been requested by a government institution that has indicated that it suspects that the information relates to national security, the defense of Canada, or the conduct of international affairs, or if the disclosure is requested for the purpose of enforcing any law of Canada for which it is responsible. Likewise, the section enables bodies subject to the law to voluntarily disclose information to the law enforcement agencies if they suspect that the information concerns national security, the defense of Canada, or the conduct of international affairs.

Section 9(2) provides that a body asked by an individual to inform him when his information is disclosed to a government institution is obliged to inform the government institution concerned regarding the request, and that institution is entitled to prohibit the body from complying with the request if it has reasonable cause to believe that complying with the request will harm national security, the defense of Canada, or international relations.

On the criminal level, the Criminal Code[210] provides that, as a rule, search warrants are required to conduct searches; however, a law enforcement official is entitled to conduct a search of a person, vehicle, or premises (which are not used as residences) without a search warrant if he has reasonable cause to believe that they unlawfully contain weapons or explosives and the conditions for obtaining a search warrant exist but because of the urgency of the matter he is unable to obtain it.[211]

Likewise, the Criminal Code states that the law enforcement agencies

209. Beginning in January 2004, the Act is due to broaden its application to all private bodies that collect, use, or transmit personal information as part of their commercial activities. *See id.* § 30.

210. Criminal Code, R.S.C. 1970, c. C-46.

211. Criminal Code § 117.02.

are entitled to monitor private communications[212] by virtue of a search warrant, which shall not be given unless the court is persuaded that "other investigative procedures have been tried and have failed, other procedures are unlikely to succeed or the urgency of the matter is such that it would be impractical to carry out the investigation of the offence using only other investigative procedures."[213]

The severity of the infringement to the privacy of a person being monitored has led the court to hold that the appropriate balance between the public interest in the proper conduct of criminal investigations and the right of the individual to privacy requires a stringent interpretation of the above requirements.[214]

Monitoring without a warrant is only possible in cases where there is reasonable cause to believe that immediate monitoring, which does not leave time to apply for a judicial warrant, is essential to prevent the commission of an offense likely to cause serious damage to a person or property.[215]

The rules applicable to the Canadian Security Intelligence Service when gathering information are set out in the Canadian Security Intelligence Service Act.[216] The intelligence service is empowered to gather information concerning activities that give reasonable cause to suspect that they may endanger the security of Canada (such as espionage and the threat to commit violent acts against people or property with the purpose of promoting political, religious, or ideological objectives).[217] The information must be gathered under a judicial search warrant,[218] which will only be issued upon proof of reasonable cause for belief that the surveillance activities are essential for a security investigation or to fulfill the duties of the service, or after proving that other investigative means have been tried and have failed or cannot be expected to succeed, or that because of the urgency of the investigation using any other techniques to gather information would lead to the investigation being thwarted, or that failure to issue the warrant would mean that information necessary for ensuring the security of Canada or fulfilling the functions of the service

212. Section 183 of the Criminal Code defines private communication as follows: "Private communication" means any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.

213. Criminal Code § 186.

214. R. v. Araujo, 2 S.C.R. 992 (2000).

215. Criminal Code § 184.4.

216. Canadian Security Intelligence Service Act, R.S.C., 1985, c. C-23.

217. Canadian Security Intelligence Service Act §§ 2, 12.

218. Canadian Security Intelligence Service Act (RE) (T.D.), 1 F.C. (Ottawa) 420 (1998).

would not be gathered.[219]

Likewise, the Act sets out the circumstances in which the service is entitled to transfer to various bodies information in its control;[220] for example, when this is necessary to fulfill its functions or when the information relates to international relations or to the defense of Canada.

The Emergencies Act[221] provides that when a state of international emergency[222] has been declared, it is possible to enter and search any vehicle or premises (including a residential home) and search any person found therein—without a search warrant.

Under the influence of the attack of September 11th, Canada—like the United States—believed that the existing balance between human rights and security needs left it with insufficient tools to effectively fight terrorism.[223] The tragedy that had struck its neighbor, as well as the desire to ensure that it itself would not fall victim to a similar disaster, led to the enactment of the Anti-Terrorism Act, Bill C-36, less than three months after the attack on the United States.[224]

The provisions of the Act significantly expand the powers of the government while concurrently restricting many of the freedoms and rights of the individual, including the right to privacy.

Concurrently with a vague definition of the acts that are deemed to be terrorist acts, the law significantly broadens the investigative powers of the law enforcement agencies and limits the access of the individual to information on grounds of national security. Thus, for example, in amending the criminal code, the Act states as follows: *first*, every Canadian citizen or permanent resident must report to the authorities immediately upon becoming aware that he is holding property that belongs to a terrorist organization or to someone on its behalf, and he is also obliged to report any transaction or commercial offer relating to that property.[225] *Second*, a number of bodies, including foreign banks operating in Canada and credit companies, must carry out routine checks to ascertain whether they are holding property belonging to a terrorist organization or someone acting

219. Canadian Security Intelligence Service Act § 21.

220. Canadian Security Intelligence Service Act § 19.

221. Emergencies Act, R.S. 1985, c. 22 (4th Supp.), § 30(1)(d).

222. A state of international emergency is defined as follows:

"'International emergency' means an emergency involving Canada and one or more other countries that arises from acts of intimidation or coercion or the real or imminent use of serious force or violence and that is so serious as to be a national emergency." Emergencies Act § 27.

223. K. Roach, *Did September 11 Change Everything? Struggling to Preserve Canadian Values in the Face of Terrorism*, 47 McGILL L.J. 893, 895 (2002); S.J. Toope, *Fallout From "9-11": Will a Security Culture Undermine Human Rights?* 65 SASK. L. REV. 281, 287 (2002).

224. Bill C-36, An Act to Amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and Other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism, 1st Sess., 37th Parl., 2001 (Assented to Dec. 18, 2001, S.C. 2001, c. 41) (hereinafter Bill C-36).

225. Criminal Code § 83.1 (as amended by Bill C-36).

on its behalf. These bodies must report their findings periodically.[226] *Third*, the Act empowers the courts to issue search warrants of premises if they are persuaded of the existence of reasonable cause to suspect that they contain property that is subject to confiscation under the law.[227] *Fourth*, whereas, as noted, the Criminal Code establishes a strict standard for issuing a wiretap warrant within the context of an investigation of ordinary criminal offenses, the amendment provides that when the wiretap is sought within the context of an investigation of terrorist offenses, a much easier standard must be met, which only requires proof that the sought after wiretap is the most effective means in the circumstances of the case.[228] *Fifth*, the Act provides that within the context of a terror investigation, a judge is entitled to issue an order in an "investigative hearing" that requires every person to answer questions and hand over articles in his control, unless these acts infringe the duty of secrecy owed by that person under law.[229]

In amending the National Defense Act, the bill provides that it is possible to monitor private communications without a judicial warrant, upon authorization by the Minister of Defense, if the sole purpose of monitoring is to gather foreign intelligence, and on condition that it is directed at an alien located outside Canada, that there is no reasonable possibility of acquiring the information by other means, that the information is likely to be of great value, and that sufficient means were taken to ensure the privacy of the citizens and residents of Canada and to ensure that the information would only be used to the extent necessitated by security needs, the defense of Canada, and international relations.[230]

Likewise, the Minister is empowered to monitor private communications, if the sole purpose thereof is to protect the government's computer systems and networks, and on condition that monitoring is essential to protect the computer systems and networks, that there is no reasonable possibility of acquiring the information by other means, that there is no reasonable possibility of obtaining the consent of people who are likely to be the subjects of the monitoring, and that the necessary steps were taken to ensure the privacy of the citizens and residents of the state and to ensure that the information would only be used to the extent necessary to achieve the objective of the monitoring.[231]

In amending the Money Laundering Act,[232] the bill provides that upon the existence of reasonable cause to suspect an attempt to smuggle financial resources in or out of the country, a police officer is entitled to search transport vehicles, cargo, or mail entering or taken out of the jurisdiction of the state.

---

226. *Id.* § 83.11 (as amended by Bill C-36).
227. *Id.* § 83.13 (as amended by Bill C-36).
228. *Id.* § 186 (1.1) (as amended by Bill C-36).
229. This provision is in force until December 31, 2006, save if it will be extended prior thereto. *Id.* §§ 83.28, 83.32 (as amended by Bill C-36).
230. National Defense Act, R.S. c. N-5 § 273.65(1)(2) (as amended by Bill C-36).
231. *Id.* § 273.65(3)(4) (as amended by Bill C-36).
232. Proceeds of Crime (Money Laundering) and Terrorist Financing Act, 2000, c. 17, §§ 16, 17.1 (as amended by Bill C-36).

In amending the Privacy Act and the Personal Information Protection and Electronic Documents Act, the bill provides that a person may not see the information relating to him held by the bodies subject to these Acts where a certificate of privilege has been issued prohibiting disclosure of the information.[233] Likewise, the bill states that the certificate of privilege precludes the disclosure of information under the Access to Information Act.[234]

C. United Kingdom

Despite possessing a democratic tradition that has evolved over hundreds of years, the United Kingdom has refrained from entrenching its commitment to individual rights and freedoms in a written constitutional document.

In 1998, Parliament passed the Human Rights Act, which gave domestic effect to the provisions of the European Convention on Human Rights.[235] Thus, the right to privacy, which is explicitly protected in Article 8 of the Convention, acquired binding legal force.[236]

A number of statutes protect various aspects of the right to privacy; the most important of these is the Data Protection Act,[237] which establishes the legal regime for data held by public and private bodies. According to the Act, these bodies must register the type of data held by them, the purpose for collecting the data, and their use with the Office of the Information Commissioner—an independent public body that is responsible for managing the register and enforcing the statutory provisions. Likewise, the Act grants every person the right to request notification whenever action is taken to collect or use data relating to him, and prohibits the bodies subject to the Act from collecting, using, or disclosing data outside the framework of the means and purposes established for collecting and managing it. However, these provisions do not apply when to do so would harm national security.[238]

In the year 2000, the Regulation of Investigatory Powers Act was passed.[239] This Act grants the investigatory bodies extremely broad pow-

233. Privacy Act, R.S. 1985, c. P-21, § 70.1 (as amended by Bill C-36); Personal Information Protection and Electronic Documents Act § 4.1 (as amended by Bill C-36).

234. Access to Information Act, R.S. c. A-1, § 69.1 (as amended by Bill C-36).

235. Human Rights Act, 1998, c. 42.

236. *Id.* Article 8 of the Convention provides as follows:

Right to Respect for Private and Family Life

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.

237. Data Protection Act, 1998, c. 29.

238. *Id.* §§ 7, 17, 28, 55.

239. Regulation of Investigatory Powers Act, 2000, c. 23.

ers, without the need to obtain judicial warrants. The extent to which this Act is compatible with the provisions of the European Convention on Human Rights is open to grave question. Thus, inter alia, the Act enables the Secretary of State for Defense to authorize the interception of communications transferred by means of the postal service or telecommunication systems, if this is necessary for reasons of national security, as part of the investigation of serious crimes or to safeguard the economic well-being of the United Kingdom.[240] Likewise, the Act enables the Defense Secretary to require these service providers to adjust their systems to enable this monitoring to take place.[241]

Section 22 enables orders to be issued to these service providers to disclose identifying communication data—as opposed to content information—to the legal authorities relating to the users of their services, if this is necessary, inter alia, on grounds of national security, public safety, the investigation of serious crime, or safeguarding the economic well-being of the state. Likewise, the Act enables the Defense Secretary or other authorized officials to authorize human surveillance on grounds of national security.[242] Section 49 provides that it is possible to demand any person who is in possession of the key to any encoded electronic address to disclose it to the authorities if reasons of national security, public safety, investigation of serious crime, or safeguarding the economic well-being of the state so require.

A number of statutes grant the police wide powers to search the body and premises of a person. Thus, for example, Section 1 of the Police and Criminal Evidence Act enables a constable to search any vehicle or person located in a public place, without a search warrant, if he has reasonable cause to suspect that weapons, explosives, or equipment intended for use in the commission of a crime are unlawfully present there.[243] Section 8 authorizes a justice of the peace to issue a search warrant for premises if he is satisfied that there are reasonable grounds for believing that a serious arrestable offense has been committed and that there is material in the premises that is likely to be of "substantial value" to the investigation of the offense.

Section 17 authorizes a constable to enter and search any premises to arrest a person for an arrestable offense, where he has reasonable grounds for believing that the person whom he is seeking is on the premises. Similarly, Section 18 authorizes a constable to enter and search any premises occupied by a person who is under arrest for an arrestable offense, without a search warrant, if he has reasonable grounds for suspecting that there is on the premises evidence that relates to that offense; or to some other arrestable offense connected with or similar to that offense. Section 60 enables police commanders to authorize their subordinates to search every

240. *Id.* § 5.
241. *Id.* § 12.
242. *Id.*§§ 26-45.
243. Police and Criminal Evidence Act, 1984, c. 60, § 1.

vehicle or person located in a cordoned area, where there is reasonable cause to believe that serious violent offenses will be committed there.

In the year 2000, the Terrorism Act was passed, incorporating numerous provisions that significantly infringe the right to privacy.[244] Thus, for example, Section 19 provides that a person commits an offense if he does not disclose to a constable as soon as is reasonably practicable that information has come to his attention in the course of his business leading him to reasonably suspect that another person is supporting terrorists financially, is assisting in obtaining financial support, is performing actions aimed at money laundering for terrorist purposes, or knowingly holds property intended for terrorist purposes. Section 20 permits—but does not compel—a person to disclose to a constable that he suspects that money or other property is terrorist property, and Section 21 provides that a person who participates in activities supporting terrorist acts as aforesaid shall not be liable for his involvement therein if he makes a disclosure on his own initiative to the police immediately after suspecting that he was involved in prohibited activities.

Likewise, the Act states that during the course of terrorist investigations, a constable may apply for a judicial warrant authorizing him to search premises and any person found therein. The judge may only give this order if he is persuaded that there is reasonable cause to believe that in the said premises there are articles of substantive value in advancing the investigation and that the grant of the warrant is essential in the circumstances.[245]

In addition, during the course of investigating terror, a judge is entitled to issue an order requiring a financial institution to divulge defined customer information in its possession, such as the customer's account number, full name, date of birth, address, and the date on which the financial institution and the customer begins or ends a business relationship. The order will only be granted on proof that the order will enhance the effectiveness of the investigation.[246] Section 39 of the Act provides that where a person knows or has reasonable cause to suspect that a constable is conducting or proposes to conduct a terrorist investigation, the person commits an offense if he discloses to another anything that is likely to prejudice the investigation.

Section 42 provides that a judge may on the application of a constable issue a warrant for specified premises if he is satisfied that there are reasonable grounds for suspecting that a person whom the constable reasonably suspects to be a person who is or has been concerned in the commission, preparation, or instigation of acts of terrorism is to be found there.

Likewise, the Act provides that a constable may arrest without a warrant a person whom he reasonably suspects to be a terrorist; moreover, he

244. Terrorism Act, 2000, c. 11 (the Act came into force in February 2001).
245. *Id.* § 37.
246. *Id.* § 38.

may search a person arrested under Section 41 to discover whether he possesses anything that may constitute evidence that he is a terrorist. A constable may also search a person suspected of being a terrorist, even without arresting him.[247]

A particularly draconian power set out in the law enables police commanders to authorize constables to search every vessel or person located in a defined area, if they believe that this is expedient to prevent acts of terrorism. Even though this power allows the invasion of the privacy of people who are not suspected of having committed any offense, the Act does not require prior judicial scrutiny or even retroactive scrutiny, of the exercise of the power. Only two restrictions are imposed on this power: first, that the commander reports the grant of authorization to the Secretary of State for Defense as soon as is reasonably practicable—the Secretary of State may then modify or cancel the authorization; second, that the authorization will be valid for a maximum period of 28 days, following which it must be renewed in a new process.[248]

The terrorist attack on the United States also had an impact on the United Kingdom. Like the governments of the United States and Canada, which hastened to initiate legal legislative action clearly according superiority to security interests over individual rights, the United Kingdom also believed that the balance of interests established in its statutes failed to provide it with sufficient tools to defend the country against terrorists,[249] and consequently, even though only a few months had elapsed since the Terrorism Act entered into force, the Anti-Terrorism, Crime and Security Act was passed.[250]

Among its provisions, the latter Act broadens the range of customer information that financial institutions must divulge under the Terrorism Act to also include information regarding the customer's account in that institution.[251]

Section 17 of the Act expands the duty of disclosure of certain public authorities to cases where the information is sought in the context of an investigation or criminal procedure.

Section 19 permits the tax authorities to voluntarily disclose information in their possession, if such disclosure is not prohibited under the Data Protection Act, to facilitate the carrying out by any of the intelligence services of any of that service's functions or for any criminal investigation or criminal proceedings.

---

247. *Id.* §§ 41, 43.

248. *Id.* §§ 44-46.

249. See the explanatory notes to the Act, prepared by government offices: "The purpose of this Act is to build on legislation in a number of areas to ensure that the Government, in the light of the new situation arising from the September 11 terrorist attacks on New York and Washington, have the necessary powers to counter the threat to the UK," *at* http://www.hmso.gov.uk/acts/en/2001en24.htm (last visited Aug. 10, 2003).

250. Anti-terrorism, Crime and Security Act, 2001, c. 24.

251. *Id.* § 3.

The Act also provides that a judge may issue a warrant to search premises if he is satisfied that there are reasonable grounds for suspecting that evidence of the commission of nuclear, chemical, or biological weapons related offenses is to be found on any premises. The power to search premises includes the power to search any persons present therein as well as those suspected of concealing evidence connected to the commission of the aforesaid offenses.[252] Other statutory provisions require all persons to inform the Secretary of State for Defense of their intention to keep dangerous substances on their premises. The police are authorized to require all persons holding such substances to inform them of the security measures taken when handling them, as well as the identity of persons having access to the substances or to the premises in which they are kept. Likewise, the police are entitled to enter and search premises in which dangerous substances are held to ensure the security of the substances.[253]

In addition, the Act enables the Secretary of State to establish procedures relating to the retention of communications data to safeguard national security, to prevent or detect crime, or to prosecute offenders that may relate directly or indirectly to national security.[254]

D. The European Union

The institutions and powers of the European Community are set out in the line of conventions that established the Community.[255]

Its activities are based on primary legal sources (public international law, Community treaties, treaties between the Community and foreign states and supraprinciples relating to human freedoms and rights), as well as secondary legal sources (regulations, directives, and decisions).

Both in areas of jurisdiction transferred by the member states to the Communities and in areas reserved by them, the states are committed to complying with the rules of public international law. However, special restrictions apply to those matters transferred to the jurisdiction of the Community, as these cannot contradict the constitutional traditions common to the member states, as established by the international treaties to which the Community is a party or to which the member states are party.[256]

In this context, three treaties are particularly worthy of mention. The first is the European Convention for the Protection of Human Rights and Fundamental Freedoms, which was signed in Rome in November 1950 and which provides in Article 8 for the individual's right to respect for private and family life.[257] Second, is the Treaty on the European Union, which

252. *Id.* § 52.
253. *Id.* §§ 59-61, 65.
254. *Id.* § 102.
255. E. Lev, The Law of the European Community 21 (1994).
256. The European Union and Human Rights 5-13 (N.A. Neuwahl & A. Rosas eds., 1995); Case 4/73 Nold v. Commission 491 (1974).
257. The European Convention on Human Rights (1950), *at* http://www.hrcr.org/docs/Eur_Convention/euroconv2.html (last visited Aug. 10, 2003).

declares the Union's commitment to respect for the basic rights set out in the European Convention for the Protection of Human Rights and to conducting a joint foreign and security policy, which has as its objective strengthening the security of the Union, the security of the member states, international safety, and the democratic rule of law.[258] Third, is the Nice Convention signed in the year 2000, in which the Union declared that it is founded on principles of freedom, democracy and the rule of law and in Article 7 declared its commitment to respect for the individual's right to privacy.[259]

In a variety of directives, the Community has proclaimed its objectives on a range of legal issues within its jurisdiction. Each member state is required to adapt its domestic laws to these directives as the Community's laws in these areas supersede the states' internal laws.[260]

In October 1995, the Community issued the Data Protection Directive,[261] which was intended to harmonize the various state laws[262] relating to the gathering, processing, and disclosure–both automatic and manual–of personal information.[263] However, it is important to note that the provisions of the directive are not designed to regulate the data laws in the areas of national security and criminal law.[264]

The Directive requires the member states to establish a legal regime that will ensure the fair and legal collection and processing of personal data, for clear and defined purposes, and the establishment of appropriate regulations for data protection. Special restrictions apply to the processing of sensitive data on such matters as race, nationality, religion, health, and political and ideological beliefs. Likewise, the Directive requires the states to refrain from transferring their citizens' personal data to states that do not grant appropriate protection to personal data, and to establish an independent public body (controller) to be responsible for the enforcement of

---

258. *See* http://europa.eu.int/en/record/mt/title1.html (last visited Aug. 10, 2003).

259. The European Charter of Human Rights and Fundamental Freedoms, *at* http://www.europarl.eu.int/charter/pdf/text_en.pdf (last visited August 10, 2003).

260. Case 6/64 Costa v. Enel 585 (1964).

261. Directive 95/46/EC of the European Parliament and of the Council of October 24, 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (hereinafter Data Protection Directive).

262. See Paragraph 1 referring to the "Object of the Directive":

> 1. In accordance with this Directive, member states shall protect the fundamental rights and freedoms of natural persons and in particular their right to privacy with respect to the processing of personal data.
>
> 2. Member states shall neither restrict nor prohibit the free flow of personal data between member states for reasons connected with the protection afforded under Paragraph 1.

Id. par. 1.

263. Paragraph 2 of the Directive defines personal data as follows:

> any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.

Id. par. 2.

264. Data Protection Directive, *supra* note 261, Art. 3.

privacy laws to be enacted in the future in compliance with the provisions of the Directive.

In 1997, the Data Protection Telecommunication Directive[265] was authorized, containing restrictions on the collection and processing of data by means of telecommunication systems. Inter alia, the Directive requires the member states to enact laws prohibiting the monitoring and storage of electronic data and also limits the ability to gather identifying data. At the same time, it does not prevent the member states from establishing incompatible regulations if reasons of national security so require.[266]

Following the events of September 11th, many of the member states of the European Union concluded that there was no choice but to take far-reaching measures, some of which entailed a significant infringement of individuals' rights, to protect Europe against similar attacks.[267] Accordingly, in July 2002, the European Parliament adopted the Electronic Communication Privacy Directive,[268] which eased a number of the restrictions on the processing of personal data in the electronic communication sector but does not bind the member states in the areas of national security and criminal law. The provisions of the Directive do not prevent the member states from enacting laws that require the providers of electronic communication services to collect and store identifying customer data for a variety of purposes.

However, concurrently, the Directive introduces an important provision protecting the individual against identification of his precise location using his cellular telephone, since it requires the communication providers to inform their customers of the nature of the data being gathered about their location and the purpose of collecting it. If the customer consents to the collection of the data, it may be collected only to the extent necessary to provide the service, and in the absence of consent, the data may only be collected on an anonymous basis.

Conclusion

We must examine the appropriate scope of protection to grant to the fundamental right to privacy in times of national emergency on the basis of our new, more acute understanding. On one hand, we must refrain from clinging to the false illusion that in such grave times of trouble it is possible to protect the individual's privacy as if that individual were living in a utopian state of peace and tranquility. The terrorists who strike at us challenge the democratic liberal paradigm on which our states are founded;

265. Directive 97/66/EC of the European Parliament and of the Council of December 15, 1997 on the Processing of Personal Data and the Protection of Privacy in the Telecommunications Sector.

266. *Id.* Art. 14.

267. W. Horsley, *EU to Push Through Terror Laws*, *at* http://news.bbc.co.uk/1/hi/world/europe/1689216.stm (last visited Aug. 5, 2003).

268. Directive 2002/58/EC of the European Parliament and of the Council of July 12, 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector.

however, at the same time, they make malevolent and iniquitous use of the freedoms and rights granted to the individual by virtue of that paradigm to carry out their murderous plans. On the other hand, unlike those in the past who believed that the ideological struggle between the democratic theory and its challengers had ended with the clear victory of democracy,[269] today—after the events of the last century and in particular the transformation of Germany from a state boasting a long democratic tradition to one embracing Nazism—we can no longer delude ourselves into thinking that the ideological battle has ended and that our society is guaranteed an abiding democratic future. On the contrary, we understand the following:

> The democratic regimes throughout the world . . . are not primeval rock the existence of which is guaranteed after it is created. Without vigilance and persistent activity democracies may collapse in a gradual manner and occasionally also in the blink of an eye. We must be aware of this potential for fragility and understand that it is possible to overcome the danger only by means of openness and watchfulness and taking a firm stand on safeguarding freedoms.[270]

A comparative examination of the balancing formulae between security needs and privacy shows that even though, prior to the terrorist attack on the United States in September 2001, the states referred to in this Article had granted the security authorities broad powers to invade a person's privacy, after that attack all those countries (except Israel) engaged in hasty and far-reaching legislative changes to these formulae, which significantly limited the protection of privacy.

Is it true that the array of checks and balances that previously existed in these states limited the effectiveness of the tools available to the security authorities to fight terrorism, and that therefore the legislative changes were legitimate and inescapable measures forced on democratic states seeking to defend themselves? Or, were these measures the outcome of panic and paranoia lacking any factual basis?

An answer to these questions requires us to examine a number of points. First, the tool that most seriously denies and restricts freedoms available to a democratic state is its criminal law, and consequently the state must use the utmost care to comply with the procedural rules designed to ensure that the individual against whom this tool is directed enjoys fair process.[271] Even though security offenses are at the same time criminal offenses, the harm they cause to national security, public safety, and the fabric of social life is much more destructive. Therefore, investigative powers that cause disproportionate harm to an individual in an ordinary criminal process, such as the imposition of certain restrictions on his

269. F. Fukuyama, *The End of History?*, in CONFLICT AFTER THE COLD WAR: ARGUMENTS ON CAUSES OF WAR AND PEACE 5-18 (R.K. Betts ed., 1994).

270. S.N. Eisenstadt, DEMOCRACY AND ITS MEANDERINGS: PARADOXES IN THE MODERN DEMOCRACY 109 (Ministry of Defense Press 2002) (Heb.).

271. M.H. 3052/99 Barns v. State of Israel (as yet unpublished).

right to consult with an attorney[272] or a covert search of his premises or personal effects are acceptable as a constitutional exception in the security arena.

In situations when the Israeli legislature (and generally also the Canadian legislature) were careful to refrain from expanding the scope of application of the special security legislation to the criminal process as a whole, the legislatures of the United States and the United Kingdom, prior to the new antiterrorist acts and even more so subsequently, abstained from drawing a clear distinction of principle between the two areas. The application of the security legislation to ordinary criminal offenses does not lead rationally to achieving the purpose of the infringement, i.e., prevention of acts of terrorism and therefore violates the individual's right to a fair criminal trial in a disproportionate manner.

Second, while every power requires the establishment of effective supervisory mechanisms over how the powers are exercised to ensure that they are not improperly exploited or used unnecessarily, this requirement is even more important in security related matters, where the scope of the powers and the relative ease with which they can be exercised generate capabilities of a magnitude that greatly exceed those in any other field.[273] Moreover, the difficulty in defining the term "terror" has led every country to adopt a broad and vague definition of this concept. While there is no doubt that the purpose of the vagueness is to ensure that the term will catch such terrorist organizations as Al Qaeda and Hamas within its net, the byproduct is that many of the legitimate acts of civil protest carried out under the banner of freedom of speech and association may fall within its precincts,[274] and therefore it is conceivable that one day political opponents will pervert the purpose of the vagueness in an effort to neutralize each another.

Notwithstanding the immense potential risks, and notwithstanding that establishing restraining and controlling mechanisms (such as substantive, as opposed to symbolic, prior judicial scrutiny, or at least retrospective scrutiny, or the establishment of supervisory bodies, or the requirement of periodic reports to ensure public transparency) would not undermine the effective implementation of the powers, it is apparent that all the states have on occasion renounced these mechanisms. This is particularly true in the aftermath of the September 11th attacks. The most extreme and far-reaching renunciation of the system of checks and balances may be found in the laws of the United States (first seen in the provisions of the Anti-

272. Section 35 of the Criminal Procedure Law (Powers of Enforcement-Arrests), 5756-1996, S.H. 1592, 338.

273. Zamir, *supra* note 32, at 22.

274. For a definition "terrorist organization" and "member of a terrorist organization" in Israel, see the Prevention of Terrorism Ordinance, 5708-1948, Official Gazette, supp. A, 73; for the definition of "domestic terrorism" in the United States, see USA PATRIOT Act, *supra* note 188, § 802 (amending 18 U.S.C 2331); for the definition of "terrorism offence" in Canada, see Criminal Code, *supra* note 210, § 2 (amended by Bill C-36); and for the definition of "terrorism" in the United Kingdom, see Terrorism Act, *supra* note 244, § 1.

Terrorism and Effective Death Penalty Act and developed in the Patriot Act) and in the laws of the United Kingdom (which patently renounced judicial review in the Regulation of Investigatory Powers Act, followed by further waivers of checks and balances in the Terrorism Act and the Anti-Terrorism, Crime and Security Act).

Third, a system of balances between security and freedom has existed since time immemorial, although each era has sought to adapt those balances to the changing reality. Today, technological means are available to image the body of a person under his clothes, track his movements using satellite pictures and closed circuit cameras, pinpoint his location with the aid of beepers or cellular telephones, crosscheck vast quantities of data relating to the person to determine whether he fits the profile of a potential terrorist, track his movements on the internet, and engage in multiple other capabilities, which enable a state to create a detailed and comprehensive portrait of the lives of its citizens.

While it is inappropriate to latch on to outdated checks and balances from another era, which would prevent the security authorities from making use of technological innovations on grounds of the severe harm caused to the privacy of masses of innocent persons, the state—if it wishes to be faithful to its democratic values—cannot permit unrestrained use of these technologies, even if they have the potential to assist in the prevention of acts if terrorism. The reason for this is as follows:

> It is the fate of democracy that it does not see all means as justified, and not all the methods adopted by its enemies are open to it. On occasion, democracy fights with one hand tied behind its back. Nonetheless, the reach of democracy is superior, as safeguarding the rule of law and recognition of the freedoms of the individual, are important components in its concept of security. Ultimately, they fortify its spirit, strengthen it and enable it to overcome its problems.[275]

The more the measure violates the core aspects of privacy, the more stringent the inquiry must be into whether it meets the three tests of proportionality, i.e., (a) its compatibility with the purpose of the violation (thus, for example, a violation of the core aspect of privacy by means of technological devices of doubtful efficacy and reliability will not be allowed); (b) whether a measure exists that may achieve the same purpose by means of a less severe violation (a violation of a core aspect narrows the zone of proportionality and requires selection of the measure that causes the minimum harm); and (c) whether a reasonable relationship exists between the damage caused to the individual as a result of the infringement of his privacy (the damage is most severe on the core level) and the public benefit ensuing from achieving the security purpose.[276]

We have seen that a number of arrangements in Israeli law fail to meet these tests. Regarding comparative law, the events of September 2001 led

---

275. H.C. 5100/94 Public Committee Against Torture in Israel v. Government of Israel, 53(4) P.D. 817, 845 (Heb.).

276. D. Dorner, *Proportionality*, *in* BERENZON BOOK 281 (Vol. B., A. Barak and H. Berenzon, eds., 2000) (Heb.).

the states discussed here to sharply tilt the scales towards security needs, on the ground that until that date their checks and balances formulae had been mistaken and had given excessive weight to the individual's privacy. In my opinion, this argument is factually unfounded, as our examination of the statutory amendments has revealed that most of the amendments did not grant the security authorities new powers but rather removed or eased the oversight mechanisms of past powers—a process that does not increase the efficiency of the war against terrorism at all but only creates a danger of unlawful implementation of those powers.

At the opening of this section I referred to the fragility of democracy and therefore to the possibility that it will collapse in the absence of sufficient vigilance to ensure its defense.

Emergency times pose a dual challenge to a democracy: on one hand, it must protect its citizens and ensure their security, and for this purpose it must restrict their rights. On the other hand, the democracy must safeguard itself against blindly sacrificing the values of freedom and justice on the altar of national security.

This task is not easy, either legally or morally, because in times of crisis the individual tends to accord greater weight to the collective interest in security than to individual rights. The legislature—which is an elected body dependent upon public support—is likely to exploit this temporary public mandate to engage in unnecessary, destructive, and irreversible violations of the individual's rights.

As democratic states, "we have always placed our trust in the fact that here the voice of the law is not silent even in the tumult of the hostility which surrounds us,"[277] and therefore we must be careful not to enact laws that turn the individual from an end into a means to achieve the security objective.

The State of Israel, which , since its establishment, has been contending with persistent security threats, and the democratic Western states, which, since September 2001, have understood that they too must live under the shadow of terrorist threats, have more than once surrendered to the temptation to see the individual as a tool and consequently to suspend his right to privacy on imaginary and factually baseless security grounds—a phenomenon that is particularly noticeable in the United States and the United Kingdom.

All those who argue that any infringement whatsoever to the privacy of a person can only be tolerated in times of crisis, and that immediately upon the arrival of a time of peace, it must be removed are suffering from self-delusion. The boundary line separating the protection of individuals' rights in times of emergency and their protection in times of peace is extremely fine and amorphous, and therefore there is a danger that unnecessary restrictions imposed in times of emergency, and their moral impact, will remain long after the cessation of that emergency, and we will find ourselves living in an abyss into which we have thrown ourselves

277. H.C. 320/80 Kawasma v. Minister of Defense, 35(3) P.D. 113, 120 (Heb.).

unnecessarily.[278]

Particularly in its hour of trouble, against the background of the roar of the cannon and the scenes of destruction, it is vital for the state to take honest stock and examine whether it has remained faithful to its democratic character and to the values for which it is fighting. Without this, at the end of the battle, when the veil of smoke lifts, we may discover that not only were the symbols of democracy destroyed by the terrorist attacks but also democracy itself.

---

278. A. Barak, Lecture entitled "Democracy, Terror and the Courts," delivered at the International Conference, Democracy v. Terror: Where are the Limits, Haifa University (Dec. 16, 2002).