In the Supreme Court
Sitting As the High Court of Justice

HCJ 3809/08
HCJ 9995/08

Before: Her Honor, President (Ret.) D. Beinisch
His Honor, President U. Grunis
His Honor, Deputy President E. Rivlin
Her Honor, Justice M. Naor
Her Honor, Justice E. Arbel
Her Honor, Justice E. Hayut
His Honor, Justice H. Melcer

The Petitioner in HCJ 3809/08: **The Association for Civil Rights in Israel**

The Petitioner in HCJ 9995/08: **The Israel Bar**

AGAINST

The Respondents in HCJ 3809/08:
1. **The Israel Police**
2. **The Military Police CID**
3. **The Police Internal Investigations Department of the Ministry of Justice**
4. **The Securities Authority**
5. **The Antitrust Authority**
6. **The Israel Tax Authority**
7. **The Minister of Justice**
8. **The Knesset**
9. **Bezeq, The Israel Telecommunications Corp. Ltd**
10. **Pelephone Communications Ltd**
11. **Cellcom Israel Ltd**
12. **Partner Communications Ltd**
13. **MIRS Communications Ltd**
14. **HOT Telecom LP**
15. **Netvision 013 Barak Ltd**
16. **012 Smile Communications Ltd**
17. **Bezeq International Ltd**

The Respondents in HCJ 9995/08:
1. **The Minister of Justice**
2. **The Israel Police**
3. **The Military Police CID**
4. **The IDF Military Police Internal Investigations Unit**
5. **The Securities Authority**

6. **The Antitrust Authority**
7. **The Israel Tax Authority**
8. **The Knesset**

Amicus Curiae in HCJ 3809/08: **The Press Council**

Petitions for the award of an order nisi

Date of Sessions:	28th Shevat, 5769 (February 22, 2009) 23rd Cheshvan, 5770 (November 10, 2009)
On behalf of the Petitioner in HCJ 3809/08:	Adv. **Dori Spivak**
On behalf of the Petitioner in HCJ 9995/08:	Adv. **Dan Hay**; Adv. **Kobi Sade**
On behalf of the First to Seventh Respondents in HCJ 3809/08 and HCJ 9995/08:	Adv. **Dana Briskman**;
On behalf of the Eighth Respondent in HCJ 3809/08 and HCJ 9995/08:	Adv. **Roxanna Scherman-Lamdan**
On behalf of the Tenth Respondent in HCJ 3809/08:	Adv. **Guy Flanter**; Adv. **Abayansh Tasma**
On behalf of the Eleventh Respondent in HCJ 3809/08:	Adv. **Jonathan Hamo**; Adv. **Asher Doga**
On behalf of the Twelfth Respondent in HCJ 3809/08:	Adv. **Amir Vang**
On behalf of the Ninth and Thirteenth to Seventeenth Respondents in HCJ 3809/08:	No appearance
On behalf of the Press Council (Amicus Curiae):	Adv. **Orna Lin**; Adv. **Vered Kinar**

JUDGEMENT

President (Ret.) D. Beinisch

The petitions, which have been joined, concern the constitutionality of some of the arrangements prescribed in the Criminal Procedure (Powers of Enforcement – Communications Data) Law, 5768-2007 that was published in the Official Gazette on December 27, 2007 and came into effect on June 27, 2008 (hereinafter referred to as "the Communications Data Act" or "the Act"), which permits the Israeli investigatory authorities to obtain communications data of telecommunications subscribers generally, as they are defined in the Communications (Telecommunications and Broadcasting) Act, 5742-1982 (hereinafter referred to as "the Communications Act").

General

1. It is common to say that we are now living in what is called the "information age," an age in which advanced technology makes it possible to transmit large-scale data in respect of the world around us immediately. Infinite information flows through various media – especially the Internet and the cellular communications related to it – providing a rapid answer to all the issues that concern us in our lives. The general public takes an active and intensive role in the flow of information and it streams data into the information market that affects different strata of the fabric of our lives.

As everyone knows, the technological age has not stopped developing merely with the creation of infrastructure for the ongoing transmission of information, and over the years modern technologies have also been created to enable gathering the information that flows in the virtual world and processing and analyzing it according to the different needs of those who have the ability to do so. Combining the ability to transmit information rapidly and the ability to gather it has given various entities – from State authorities, through private corporations to organized crime – a wide variety of tools and abilities they did not previously have.

This is also the background to the enactment of the Communications Data Act – the subject matter of the petitions – which resulted from an attempt to regulate how the various State authorities' powers to obtain communications data on Israel's residents are exercised in the course of performing their public duties, as well as to regulate how those data are kept by the authorities. This is of particular relevance in terms of how enforcement agencies follow the Act when performing their duties, and it necessitates a balance between the purpose of enforcement and the infringement of individual liberty.

2. The Communications Data Act prescribes arrangements, as detailed below, which enable investigatory authorities – the Israel Police, the Military Police CID, the Military Police Internal Investigations Unit, the Police Internal Investigations Department of the Ministry of Justice, the Securities Authority, the Antitrust Authority

and the Israel Tax Authority – to obtain communications data of telecommunications subscribers generally. According to the Act, a telecommunications subscriber is anyone who receives telecommunications service. The Act defines "telecommunications" as "broadcasting, transfer or reception of signs, signals, writing, visual forms, sounds or information by means of wire, wireless, an optical system or other electromagnetic systems." Therefore, a telecommunications subscriber is anyone who makes use of a telephone, mobile phone or computer for the transfer of messages of any type (conversations, text messages, email and the like.) This means the Act makes it possible to obtain communications data from all the communications companies – the various different cellular and line telephone companies and Internet providers. The communications data covered by the Act include subscriber data, which include the subscriber's identifying particulars, details of his means of paying for the service, the address where the telecommunications device used by him is installed and more; location data, which include pinpointing the peripheral equipment in the subscriber's possession; and traffic data, which include details of the type of message transmitted, its duration and scope, identification details of the subscriber who is the source of the message and also the subscriber to whom it is addressed, the time of the message's transmission and more. The Act clarifies that obtaining those data does not include obtaining the content of the messages transmitted. The ability to obtain the content of communications messages is limited, and it is regulated by the Secret Monitoring Act, 5739-1979 (hereinafter referred to as "the Secret Monitoring Law,") that is not subject to constitutional review here.

In brief, it can be said that the Act regulates three major aspects. The first concerns granting the relevant authorities power to obtain an *ex parte* order for obtaining communications data. The second is issuing an administrative permit, without filing a motion with a court, to obtain communications data in the cases detailed in the Act. The third is a database set up by the Israel Police to include several sets of data prescribed in the Act.

3. Two similar petitions challenge the Act, focusing on complaints related to those three arrangements (hereinafter "the petitions.") On April 28, 2008 the Association for Civil Rights in Israel filed a petition in which the Association maintains, in a nutshell, that the arrangements established by the Act to obtain communications data infringe the right to privacy disproportionately, and that the Act, as it is, is therefore unconstitutional. On November 26, 2008 the Israel Bar filed a petition aiming, in a nutshell, to limit the Act's application to those who have privilege (hereinafter referred to as "professionals,") such as attorneys and their clients, and also to restrict the ability to use the information collected under the Act as evidence in court proceedings. At a later stage the Press Council joined the first petition as amicus curiae, seeking to emphasize the harm anticipated from implementing the Act on journalists and their work because of the possibility created by some of the Act's provisions that journalists' sources would be exposed. With the State's oral consent, given during a hearing held before us on February 22, 2009, these petitions were heard as if a provisional order had been issued.

Discussion

4. The petitioners' arguments in the petitions are rooted in constitutional law, which are the foundation for the constitutional challenge against the Act. We shall therefore review their arguments according to the process of constitutional review accepted in our jurisprudence; in the first stage we shall review whether the Act does indeed infringe upon a protected constitutional right; in the second stage we shall review whether the Act meets the requirements of the Limitations Clause – whether it is for a proper purpose and whether it meets the criteria of proportionality accepted in our case law. In this latter respect we shall focus the discussion on the three main arrangements that make up the Act, which the petitioners' arguments mainly target . Alongside this, we shall consider whether the Act overall, given all of its arrangements, meets the criteria of proportionality. After all this we shall consider several other arguments made by the petitioners.

Does the Act Infringe a Protected Human Right?

The Right to Privacy in the Information Age

5. The petitioners' central complaint is that the Communications Data Act infringes the constitutional right to privacy. The right to privacy is enshrined in section 7 of Basic Law: Human Dignity and Liberty, which is titled "Privacy" and 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, or on or 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."

In light of the clear, express language of the Basic Law, it appears we need not go into the extensive case law that has elucidated these express statements for the purpose of these petitions. Instead, suffice it for us to refer to the classic definition of the right to privacy, developed by Warren & Brandeis back in 1890, as "the right to be let alone" (S.D. Warren, L.D. Brandeis, *The Right to Privacy*, 4 HARV L. REV. 193 (1890)). As was held in the past, the right to privacy "draws a domain in which the individual is left to himself, to develop his 'self,' without the involvement of others (and see HCJ 2481/93, *Dayan v. The Jerusalem District Commander*, IsrSC 48(2) 456, 471 (1994) and the references there,) and as such it is worthy of constitutional protection.

Nevertheless, given current reality it would be difficult for us to discuss the right to privacy without giving weight to the complexity of protecting it in the modern age because of the challenges that modern technology poses to the proper protection of the

right (Michael Birnhack, *The Private Domain: the Right to Privacy between Law and Technology*, at 35-36, 44-55, 57-88 (5771) (hereinafter: "Birnhack"); David Brin, *The Transparent Society – Will Technology Force Us to Choose between Privacy and Freedom?*, at 3-26 (1998)).

On one hand, it is clear to everyone that modern technological resources give those with access to them – be they the State or private individuals – numerous very sophisticated tools to penetrate a person's private domain that used to be considered almost inaccessible: means of surveillance and identification, computerized search methods and organized data collection in electronic databases. On the other hand, at the same time technology also provides tools that make greater protection of privacy possible, enabling the blurring of identity in the virtual domain and the performance of acts in the real world that used to necessitate complete exposure: from economic interactions through to the creation of virtual, interpersonal connections. For us, this complexity means an ambivalent attitude to the adoption of such technologies and their role in protecting the constitutional right to privacy. Moreover, it is not unusual these days to hear arguments that the behavior of individuals in the information age can be regarded as their implied waiver of privacy rights. This is in light of a *prima facie* informed choice by individuals in society to conduct social, political and economic interaction over the Internet and cellular communications, with clear knowledge of the potential exposure of that information (see further, Birnhack, at 267). It should be noted that only recently the significance of this implied waiver arose in a decision by the United States Supreme Court that came down on January 23, 2012 (*United States v. Jones*, hereinafter: "Jones," available at http://www.supremecourt.gov/opinions /11IsrSCf/10-1259.IsrSCf). All these aspects demonstrate to us the complexity of imposing constitutional balances and delineating the boundaries of the right to privacy in the present age. We have borne this complexity in mind when ruling on the petitions.

The complexity of positioning the boundaries of protection of privacy is particularly highlighted against the background of the "concern about excess power of the State, which may gather together under its control extensive information about citizens and residents and may abuse such information" (Then Justice A. Grunisin HCJ 8070/98, *The Association for Civil Rights in Israel v. The Ministry of Interior*, IsrSC 58(4) 842, 856 (2004)). This concern increases as the government gains more sophisticated means, making more extensive infringement of privacy possible. On the other hand, it is also clear that modern technology is a vital, important tool in the hands of the government, a tool that significantly assists the government in performing its duties. In fact, barring the authorities from making reasonable, balanced use of technological tools available to them could significantly impair their ability to perform their law enforcement duties. This is because technological progress and the tools that it develops are not only in the authorities' possession but are also extensively used by both small and large criminal groups that long ago realized their advantages strongly facilitate their objectives (see also Birnhack, at 175-176). In this technological battle, which continues to be waged, he who lags behind is likely to have the lower hand. It can therefore be said that the authorities must almost certainly keep their hands on the

technological pulse and rapidly adopt advanced tools and systems to help them do their work.

We considered this complexity in the past in a discussion that was focused on the proper regulation of the laws of search regarding "intruding" into one's computer:

> ""Needless to say that due to the potential infringement of the individual's rights when intruding into computer material, such regulation is essential and therefore ought to be completed soon. In the present era, computers have become a prime work tool and means of communication and an almost infinite archive that stores one's memories, the fruits of his work and his negotiations (as to the potential infringement of one's rights when intruding into computer material, see Sharon Aharoni-Goldenberg, *Hacking into Computer Systems – the Ideal and Actual Scope of the Offense,* THE DAVID WEINER BOOK ON CRIMINAL LAW AND ETHICS 429 (2009) (hereinafter: 'Aharoni-Goldenberg'). At the same time, the intensive use of computers also makes them a treasure trove of incriminating evidence and relevant information that can and should be used by investigatory authorities in their battle against lawbreakers and criminals. The complexity and sensitivity of the subject makes it necessary for the Act's adaptation to technological innovation and the potential harm that follows technology, to be undertaken not only seriously and responsibly but also with due speed" (CrimLA 8873/07, *Heinz Israel Ltd v. State of Israel*, (unreported, January 2, 2011) para. 17 of the opinion).
>
> The statement is also apt herein.

The balance between these extremes – the concerns of government's over-intrusion into the individual's life, on the one hand due to increased technological capabilities, and the importance of recognizing the advantages that technological resources provide as a means to ensure security and public order, on the other hand – is what lies at the heart of the petitions herein. Making these balances is undoubtedly intricate. In our opinion we shall examine whether the balance the legislature reached in the Act's arrangements meets the constitutional criteria recognized in our legal system.

In this context we would mention that this complexity – which affects the right to privacy in the modern era – is certainly not specific to Israel, and many countries seek to contend with it. As mentioned, as recently as January 23, 2012 the United States Supreme Court decided *Jones*, which is important to this issue. In that case the question that arose was whether attaching a GPS tracking device to a person's private vehicle amounted to a search, which is protected by the Fourth Amendment to the United States Constitution. The United States Court unanimously held that the search violated the Constitution and that an appropriate judicial order was therefore necessary. Nevertheless, the Justices were split on the proper criterion for the application of the Fourth Amendment – whether it should be in the context of the doctrine of trespass under common law (the majority opinion) or in the scope of the criterion adopted in

Katz v. United States, 389 U.S. 347, namely the "reasonable expectation of privacy" (the minority). The ability of different criteria to adapt to the changing technological environment that makes the physical dimension underlying the search less relevant given the technological surveillance capabilities that the authorities currently possess was, among other things fundamental to the difference in opinions between Justices.

6. We would also mention the important protection of the right to privacy provided by the Protection of Privacy Act, 5741-1981, which preceded the Basic Law and prohibits infringement of privacy. Although the Protection of Privacy Act expressly provides that a security authority is immune from responsibility under that statute, the exemption is limited to "an infringement reasonably committed in the course of their functions and for the purpose of carrying them out" (section 19(b) of that Act.)

Infringement of the Right

7. The Act relevant to these petitions makes it possible, as noted, to obtain communications data relating to the conversations between a subscriber and other parties, the type of messages that the subscriber transmits, their scope, duration and more. In fact, as its language additionally reflects, the Act permits obtaining all the information concerning the message transmitted, other than its contents. In addition, the Act allows obtaining extensive information about the subscriber, independently of the message he transmitted – the subscribers' current location (looking back and to the future), address, the means of payment used to purchase the device in his possession and more. In its general wording the Act allows obtaining communications data about any person involved in an offense, whether he is the victim, suspect or someone else who can lead investigatory entities to a clue. Moreover, though incidentally, the scope of the powers granted by the Act includes the authority to obtain other communications data relating to other individuals who are not necessarily involved in any offense, with whom the person who is involved in the offense has been in touch.

On its face, reviewing the powers granted by the Act suffices to reach the conclusion, which even the State does not dispute, that the Act indeed violates the constitutional right to privacy. Clearly, in surveillance of a subscriber, the investigatory authority can observe his habits in using a mobile phone, a computer or the Internet and thereby locate his social network and his activity both during working hours and in leisure time. Even assuming that the surveillance is justified and even if the subscriber is somehow involved in an offense that should be prevented, there is no doubt that his privacy is infringed when his moves are studied in such a way. Clearly, the surveillance of someone, even for the purpose of a criminal investigation, can reveal other details, the knowledge of which constitutes an infringement of the person's privacy, such as health problems, consumption habits, sexual preferences and the like. The very knowledge of them infringes the person's privacy after the data is obtained and they certainly have potential to infringe his privacy when they can be used for the purposes of investigation. This is also the case in respect of third parties with whom the individual involved in the offense has any contact. In their petition, the petitioners draw a scenario similar to that described by George Orwell in 1984. Even without finding

that we have already reached such a horrifying scenario, there is no doubt that the feeling of surveillance – the knowledge that the investigatory authorities are watchful and can scrutinize anyone, anywhere and at any time – has a disciplining effect on a person's behavior even in the private domain (Michel Foucault, *Discipline and Punish: the Birth of the Prison*, 195-228 (1977); Bart Simon, *The Return of Panopticism: Supervision, Subjection and the New Surveillance*, 3(1) Surveillance and Society 1-20 (2005)). Such being the case, it appears that we can assume that the Communications Data Act does indeed infringe upon the constitutional right to privacy.

8. As to the extent of the Act's infringement of the right to privacy, the petitioners compare the infringement of privacy caused by the Act and that caused by the Secret Monitoring Act. According to them, the infringement is on a similar scale, which, in the appropriate cases, necessitates a comparison between the various arrangements in the Secret Monitoring Act and the Act relevant to these petitions. The State again emphasized to us that, in its view, the comparison is not appropriate and that the infringement caused by the Communications Data Act is not similar to that caused by the Secret Monitoring Act. Thus, it was explained, for example, that the Communications Data Act does not permit actual listening to conversations or reading written transmitted messages, while the Secret Monitoring Act allows far greater exposure of one's privacy. According to the State, the infringement caused by the Communications Data Act is more akin to that caused by search warrants and production orders of different types.

It seems that the State's position is accepted in other legal systems. Thus, for example, American legislation distinguishes between four basic categories of electronic surveillance (see the Electronic Communications Privacy Act 1986 (ECPA) established by Chapter 18 of the United States Code (hereinafter: "USC"), the first category, and the greatest infringement of privacy, is secret monitoring (which is regulated by Chapter 1 of the ECPA). The other categories are perceived as constituting lesser infringements of privacy: electronic tracing devices (which in certain respects provide information similar to location data in the Israeli statute) are perceived as infringing privacy less than secret monitoring; obtaining data from communications service providers (similar in part to subscriber data in Israel) is a category whose infringement is even lower (the obtaining of which is regulated by the Stored Communications Act, which is part of the ECPA); and finally what are known in American law as pen/trap taps (electronic surveillance devices that make it possible to obtain data in real time about telephone numbers that have been dialed and received on a particular telephone device) that are defined as the least infringing surveillance category. In this context we would first note that the United States Patriot Act (2001) extended the definition to additionally include data about Internet addresses. Second, American courts are split as to whether permitting the use of these surveillance devices also permits obtaining data on the location of cellular phones (see further: Deborah F. Buckman, *Allowable Use of Federal Pen Register and Trap and Trace Device to Trace Cell Phones and Internet Use*, 15 ALR Fed. 2d 537 (2006)). This difference in the extent of the infringement is demonstrated in different arrangements formulated in American law for the different categories' application, which include looser requirements as the infringement caused

is mitigated. The same is the case regarding different data that can be obtained from communications providers under the Stored Communications Act mentioned above, which sets different arrangements depending on the type of data sought and distinguishes, for example, between identification data, which can also be obtained through an administrative subpoena (§2703(c)2, Chapter 18 of the USC), and the contents of transmitted messages, which require a search warrant with judicial authorization (§2703(a)(b)). Thus, according to American law's approach, in light of the relatively limited infringement caused by obtaining data through surveillance devices of the pen/trap taps type, it was held in *Smith v. Maryland*, 442 US 735, 745 (1979) that individuals have no inherent expectation of privacy in the telephone numbers that they voluntarily dial. Consequently, it was held there that a motion to obtain such data cannot be considered a "search," as protected by the Fourth Amendment to the Constitution and therefore investigatory authorities need not meet the requirements necessary for obtaining a search warrant. Nevertheless, as stated above, on January 23, 2012, the United States Supreme Court unanimously held in *Jones* that fitting a GPS tracking device to one's private motor car and monitoring his movements for 28 days did constitute a "search" that is protected under the Fourth Amendment to the Constitution and therefore did necessitate an appropriate judicial order. English law also draws a similar distinction in protecting content data compared to communications data (see, for example, section 1 the Regulation of Investigatory Powers Act, 2000, c. 23 (Eng.) (hereinafter: "the RIPA,") which requires an order for obtaining the contents of communications, as opposed to sections 21 to 25 of the same Act that grant powers to numerous authorities to obtain other communications data.)

It should be said that the parties' positions regarding the extent of the infringement upon the right to privacy as a result the Communications Data Act impacted those parties' positions regarding the Act's arrangements and their proportionality. We have given consideration to these aspects and reached the overall conclusion that for the purposes of the petition we need not decide whether the infringement of the right to privacy in the Act is greater or less than the infringement of privacy resulting from the Secret Monitoring Act. It should not be overlooked that given modern technology, the State's position creates a somewhat artificial distinction between content data and data, the obtaining of which the Act permits, because it appears that the differences between them are not so clear (see further Omer Tene, *Look at the Pot and See What Is in It: Communications Data and Personal Information in the 21st Century*, in LEGAL NET: LAW AND INFORMATION TECHNOLOGY 287 (Niva Elkin-Koren and Michael Birnhack eds., 2011). However, for the purpose of these petitions we need only find that the Communications Data Act indeed infringes upon the constitutional right to privacy, and we do not consider it necessary to establish strict rules on the relationship between the data obtained under the Secret Monitoring Act and the data obtained under the Act subject to our review.

In any event, it is clear that such infringement in itself does not render striking down the Act as unconstitutional. Investigatory powers, like penal powers, for the most part inherently infringe protected human rights. We must therefore analyze – under our accepted constitutional system – whether the infringement of the constitutional right

which results from the Act's implementation meets the requirements of the Limitations Clause of Basic Law: Human Dignity and Liberty. Should it become clear that the infringement meets such requirements, there would be no constitutional reason to strike down the Act.

9. However, before moving on to study the conditions of the Limitations Clause, in view of the petitioners' pleas, we must also review whether alongside the right to privacy, the Act infringes other protected rights. According to the Israel Bar, In addition the infringement of privacy, the Act does infringe other rights, namely the rights embodied in the professional privileges that have been recognized by statute and case law, including the right to be represented by defense counsel, freedom of the press, freedom of association, free expression, freedom of occupation, freedom of religion and more. Naturally, the Bar devoted most of its arguments to the infringement that the Act causes, as it argues, to attorney-client privilege and to the client's right to be assisted by an attorney, even when the attorney is not at all involved in the offense.

Indeed, as a general rule, it can be said that the infringement of privilege established in statute might infringe the rights the privilege protects. Among other things, as the State also mentions in its reply from January 11, 2009, the infringement of attorney-client privilege might infringe the client's due process rights. Similarly, infringing the privilege of a journalist's source might lead to an infringement of the journalist's freedom of expression. Moreover, infringing the privilege of other professionals presumably impairs – if only to a certain extent – their professional activity. On its face, professionals' freedom of occupation is thereby also infringed because such infringement erodes their ability to assure their clients' absolute confidentiality about the very relationship with them, which is an important aspect to many clients, especially when the mere need for the professional is something that the client wishes to conceal, for example need for psychological treatment or support by the social services.

Nevertheless, according to the State, the Communications Data Act – which as mentioned, prohibits the transmission of message content – does not infringe upon the various different professional privileges (except in the case of journalists, as discussed below.) This is because obtaining data concerning the very relationship between the privileged person and the professional is not within the scope of the privilege recognized by the Israeli legal system.

10. Courts have reviewed the extent of the various different professional privileges several times in the past and have held that professional privileges essentially extend to the content of the conversations held between the professional and the privileged person but not to the very existence of a relationship with the professional. The purpose of the privilege is to allow the privileged person a realm of free communication between him and the professional. Therefore, it appears that there is merit to the State's position that, generally, when the statute does not permit obtaining the contents of the conversation it does not infringe upon the protection that the privilege affords to the privileged person. (See also on medical privilege: HCJ 447/72, *Dr Bernardo*

Ismachovitz v. Aharon Baruch, Tel Aviv and Central Investigatory Assessing Officer, IsrSC 27(2) 253, 259 (1973) (Justice Y. Sussman); on attorney-client privilege: MP 227/83, *Eliyahu Miron et al v. State of Israel*, IsrSC 45(1) 62, 79 (1983) (Judge Z Cohen); MP (TA) 1529/83, *Israeli, Yerushalmi, Cohen & Co. v. State of Israel*, DCJ 5746(3) 265 (1985), which was upheld in HCJ 301/85, *Jacob Israeli v. Israel Levy, Deputy Chief Secretary of the Tel Aviv – Jaffa District Court*, IsrSC 40(1) 159 (1986)). See also Gabriel Kling, ETHICS IN ADVOCACY 418 (2001). See also in American Law: *Baird v. Koerner* 279 F. 2d 623 (9th Cir. 1960).

It is fitting here to emphasize that professional privilege, including attorney-client privilege, is for the benefit of the client, not the professional, as has already been held:

> "The privilege in section 90 above is that of the client and is first and foremost designed to guarantee an honest and open relationship between him and the attorney when the latter's professional services are needed, without the client being concerned or afraid that matters or documents disclosed during the consultation or handling of his case will ever be used against him without his consent" (BAA 17/86, *John Doe v. Israel Bar*, IsrSC 41(4) 770, 778 (1987), Justice M. Beiski).

As for journalists, the situation is slightly different. We have already discussed the importance of free press in many decisions by this Court as well as the difference between journalism and other professions. Thus, in CFH 7325/95, *Yedioth Aharonoth et al v. Kraus et al*, IsrSC 52(3) 1, 53 (1998) Judge Y. Zamir stated that:

> "A free press is not only a necessary result of democracy but it is also a necessary condition for democracy. It is a necessary condition for a representative regime, for fair and functioning governance and for human liberty. It can in fact serve as a litmus test for democracy: there is free press, so there is democracy; there is no free press, so there is no democracy. One of the main functions of the press in a democracy is to regularly and effectively criticize and check all the state agencies, and first and foremost the government. To enable the press to perform that function properly, it must be free of supervision or other government involvement."

As the State also agreed, with regard to journalists, the very identity of the person who contacts a journalist can constitute part of journalistic privilege because it may expose the journalist's source despite the protection given to such sources. This Court, by Justice M. Shamgar, discussed the protection afforded a journalist's source in the *Tzitrin* case (MP 298/86 *Ben Zion Tzitrin v. The Disciplinary Tribunal of the Israel Bar, Tel Aviv District* IsrSC 41(2) 337 (1987)). Justice Shamgar stated there: "protection of sources of information necessary for the performance of a journalist's function, including protecting the relationship of trust on the basis of which information is given in return for assurance that the source will not be revealed, is therefore a public interest and not the particular interest of the relevant newspaper or

journalist" (id., at 358). We shall return to this relevant distinction below when we come to discuss its significance in respect to the various arrangements concerning those who have privilege.

To summarize, given the concept of privilege in our legal system, apart from the case of journalists, the petitioners were unable to demonstrate that the Communications Data Act *per se* infringes the various professional privileges created by statute and case law. To the extent that there is an infringement, it is marginal to the protected right and not at its core, which enjoys broad protection. Consequently, nor have we found it possible to show infringements to other rights intended to be protected by the privilege.

Nevertheless, and for the purposes of the discussion here, we are willing to assume the possibility of obtaining communications data about professionals also constitutes a derivative infringement of the right to privacy. Consequently, when analyzing the infringement of the right to privacy as detailed above, it is proper to review it – together with the right's derivatives by applying the Communications Data Act in light of the Limitations Clause.

The Limitations Clause

Proper Purpose

11. The purpose of the Act, as put to us by the State, is to give the Police and other investigatory authorities effective tools for the battle against crime in the developing, modern world. According to the State, the dramatic development of the modern world of communications has not passed over criminals, and the media have become a convenient platform to improve the means of communication and commission of crimes. Consequently, enforcement authorities must contend with such capabilities and at the same time improve their own. It was therefore argued that an inability to obtain communications data would place law enforcement authorities at a significant disadvantage compared to criminals, both when it comes to detection and when it comes to gathering the evidence for their prosecution. In addition, the State pleads that the purpose of the Act is to make it possible to deal with urgent situations quickly, for example when a person's life is on the line or when it is necessary immediately to find offenders who have already committed crimes. According to the State, communications data – and especially pinpointing the telephone – might save lives and significantly help the prosecution of offenders. It appears that at this level there is no dispute between the parties because, as emerges from the petitions, the petitioners also agree that the purpose of the Act is a proper one and in fact they are merely contesting some of the arrangements contained in it (and see para. 23 of the Association for Civil Rights' petition and para. 22 of the Bar's petition).

We would mention that in addition to these purposes, the State mentions another, which is to regulate the obtaining of communications data which until now, according to it, has been regulated generally and broadly in the scope of section 43 of the Criminal Procedure (Arrest and Search) Ordinance [New Version], 5729-1969

(hereinafter referred to as "the Criminal Procedure Ordinance") and internal guidelines of the Attorney General. According to the State, the Act is designed to regulate and limit investigatory authorities' use of communications data in order to reduce the infringement of human rights as much as possible. Clearly this purpose itself is also a proper one. The petitioners do not dispute this, and they also agree that the creation of a complete legal arrangement for obtaining communications data by enforcement authorities is justified (see para. 22 of the Bar's petition). Indeed, as already mentioned above, it is difficult to conceive these days of law enforcement without monitoring communications data – from locating offenders when they commit offenses, tracking them and making immediate arrangements to stop an offense while it is committed (for more see Birnhack, at 53). It is therefore possible to sum up by saying that the Communications Data Act was legislated for a proper purpose. It is also clear that the Law is not inconsistent with the values of the State of Israel.

As such, our main discussion will address the proportionality of the Act and its arrangements. The petitioners themselves concentrated their constitutional arguments on the three basic arrangements relating to the possibility to obtain a judicial order under section 3; the possibility to obtain an administrative order under section 4; and the establishment of a database under section 6. At the same time, the petitioners' case did not seek the Act's striking down as a whole, and the Association for Civil Rights even emphasized in its petition that it does not dispute its "constitutionality as a whole". Our discussion will therefore first focus on reviewing the individual arrangements challenged in the petition. We shall then also briefly discuss the proportionality of the Act as a whole, considering the mechanisms and internal balances in it.

The individual arrangements prescribed by the Law, the proportionality of which we shall discuss below, are as follows –

(a) *The Arrangements Prescribed in the Law*

Section 3 – A Judicial Order

12. Section 3 prescribes an arrangement that enables an investigatory authority, as defined by the Act, to obtain communications data by applying to the magistrates court in the jurisdiction where the investigatory unit is located or the offense for which the data sought was committed. Because of the section's importance, we shall quote it below:

> *"Order to Obtain Communications Data from the Database of a Telecommunications Licensee*
>
> 3. (a) The court may, upon a motion by a police officer authorized by the Inspector General, or by a representative of another investigatory authority (in this section referred to as "the motion"), permit by order the Police or the other investigatory authority to obtain communications data from the database of a telecommunications licensee as prescribed in the

order, if it is satisfied it is necessary for any of the purposes specified below, provided that obtaining such communications data does not infringe any person's privacy beyond that necessary:

(1) To save or to protect human life;
(2) To detect, investigate or prevent offenses;
(3) To detect and prosecute offenders;
(4) To lawfully confiscate property.

(b) Where the subscriber subject the motion is a professional, the court shall allow communications data to be obtained as provided in subsection (a) only where there are grounds to suspect that the professional is involved in the offense for which the motion is filed.

(c) The motion shall be filed in writing, and it shall be supported by a declaration under warning, or by an affidavit.

(d) All the following shall, *inter alia*, be stated in the application:

(1) The facts establishing the court's jurisdiction;
(2) Details of the identity and position of the filing party and the source of his authority to file for an order under this section;
(3) A summary of the facts and information on which the motion is based;
(4) The purposes for which the communications data are needed;
(5) The requested communications data;
(6) The period of time for which the communications data are requested, including the time period preceding the order, and – subject to the provisions at the bottom of subsection (g) – including the time period after the order (in this section referred to as "future communications data");
(7) Identifying details of the subscriber or the telecommunications installation for which the communications data are requested, if known in advance, including whether the subscriber is a professional covered by professional privilege under any law (in this Act referred to as "professional"); in this paragraph, "law" includes case law;
(8) Details of previous motions to obtain communications data regarding the same person in the same investigation file (in this section referred to as "previous motions").

(e) Privileged material, on which the information specified in subsections (d)(3) and (4) is based, shall be made available only for study by the court; the material shall be marked and returned to the moving party after it has been studied.

(f) (1) The following shall be attached to the application:

(a) Decisions of the court that heard previous motions;

(b) Copies of previous motions and transcripts of court hearings on previous motions, to the extent that those were heard by a different court.

(2) Notwithstanding the provisions of paragraph (1), the court may – for special reasons that shall be recorded – hear an urgent motion even without the documents in that paragraph, if it is satisfied that it has the information it needs in order to decide the motion.

(g) When deciding a motion and when setting the period for which the communications data will be provided, the court shall consider, *inter alia*, the need to realize the objectives detailed in subsection (a), the extent to which a person's privacy will be infringed, the severity of the offense, whether the subscriber is a professional and the kind of communications data permitted to obtain under the order. The court may set different periods for obtaining communications data according to the type of communications data it permitted to obtain, provided that the maximum period for obtaining future communications data shall not exceed thirty days from the day of the order.

(h) All the following shall be specified in an order under this section:

(1) The grounds for making the order, and for an order regarding a subscriber who is a professional – detailed grounds for making the order under such circumstances;

(2) The communications data that may be obtained under the order;

(3) Identifying details of the subscriber or of the telecommunications installation, for which the communications data were requested, if known in advance;

(4) The period of time during which communications data may be obtained under the order;

(5) The date on which the order is issued and the date on which it expires.

(i) The grounds for issuing the order, as provided in subsection (h)(1), shall not be communicated to the telecommunications licensee to whom the order applies.

(j) An order issued under this section shall be in effect for thirty days from the day of its issue.

(k) The provisions of this section shall not limit the court's power to grant additional orders in the same investigation."

As can be seen, this comprehensive arrangement was established in primary legislation and it details the procedure of issuing a judicial order granting permission to obtain communications data. According to the arrangement, representatives of the competent authorities may request a communications data order from a court in the cases listed in the section. The particulars of the motion, and the factors that the court ruling on the motion must consider, are detailed and include reference to preventing unnecessary infringement of the right to privacy of the person for whom the order is sought and that of others.

13. The petitioners' arguments as to this arrangement are essentially twofold. Firstly, they maintain the objectives defined in sections 3(a)(2) and 3(a)(3) are overly broad. The petitioners ask us to read into these sections a restriction whereby the goal of a judicial order under the Act can be the investigation of a particular, specific offense or the detection of an offender who has committed a particular offense, rather than general intelligence activity to be used by the investigative authorities in their regular work of detecting offenses and offenders. Second, the petitioners assert that applying the arrangement to misdemeanors violates the proper balance between infringing the right to privacy and the proper public interest of preventing dangerous crime, and the section should therefore only be applied to offenses that are a felony.

In its reply to the petitioners' arguments, the State argued generally that the Act, including the arrangement now being discussed, is balanced, detailed, proper and practical, and that it improves, rather than violates, the protection of privacy. This is essentially considering the situation before the Act came into effect, when investigatory authorities could request communications data from communications companies with a court's order to produce documents issued according to section 43 of the Criminal Procedure Ordinance upon the request of investigatory entities. The State explains that the legislature was aware of the possibility of infringing the right to privacy but, according to it, the current Act includes mechanism to properly protect citizens against disproportionate infringement of their rights. With reference more specifically to the petitioners' first argument, the State asserted that it did not consider additional conditions to the Act's sections to be justified. This is because, according to the State, the sections of the Act in any event require demonstrating a concrete suspicion in order to file the motion. Thus the petitioners' concern about a general motion that involves no suspicion is dispelled. The mandatory reports to the Knesset also limit the petitioners' concern. We shall consider the petitioners' arguments in order.

The Breadth of the Grounds for Issuing a Judicial Order under Section 3

14. According to the language of sections 3(a)(2) and (3) they do *prima facie* permit the investigatory authorities to act in the broadest of circumstances. According to those sections, when issuing an order the court may consider general objectives, like detection of offenses or detection of offenders. The acts specified in subsections (1) to (4) do in fact define all the functions of the investigatory authorities, and thus under the language of the Act the court may therefore issue an order to obtain communications data regarding any activity by such authorities. This arrangement meets the first

requirement of proportionality because it maintains a rational connection between the objective of preventing crime and detecting and penalizing offenders. Nevertheless, the arrangement does create several difficulties in terms of the second proportionality requirement. In other words, does the arrangement in section 3 of the Act constitute the least restrictive means of those available to the investigatory authority. According to the petitioners, the purpose of the Act can be achieved by taking less restrictive means: exercising the power prescribed in sections 3(a)(2) and 3(a)(3) only in cases where the communications data is requested for detecting a particular offense or a specific offender, as opposed to general intelligence activity for detecting offenses or offenders.

15. According to the petitioners, such a limiting requirement can be read into the Act under the doctrine known (essentially in Canadian law) as "reading in". This doctrine seeks to read into the statute under judicial review a provision that will cure its unconstitutionality (on "reading in" see: Aharon Barak, INTERPRETATION IN LAW, PART THREE – CONSTITUTIONAL INTERPRETATION 763 (5754), hereinafter: "Interpretation in Law", HCJ 8300/02, *Gadban Nasser v. Government of Israel* (unpublished, May 22, 2012 (hereinafter: "Nasser") paras. 55-60). It should first be said that the use of this tool is not the appropriate way to limit the arrangements in the Act as the petitioners seek. The use that is generally made of this doctrine has sought, in the name of the principle of equality, to apply the statute under review to categories the legislature omitted, reading new categories into the statute, all within the legislative purpose. This was done, for example, in HCJ 721/24, *El Al Israel Airlines Ltd v. Jonathan Danilevitz*, IsrSC 48(5) 749 (1994) (hereinafter: "Danilevitz"), when a new category – same-sex couples – was introduced into the beneficial collective agreement (and see Danilevitz, p. 764-67 and sources there; Interpretation in Law, *Id.*; see also *s*, para. 60). Our case is different. In the circumstances of the Act, we are not faced with a question of preferring certain categories to categories to which the Act, according to its plain language, does not apply, and we have no interest in infringing equality. Even the petitioners do not indicate such infringement. We therefore do not believe the doctrine of "reading in", with all its implications, should be applied in the present circumstances. At this time, when the Act is before us at first instance, we must make use of the inherent tools at the Court's disposal – interpretation of the statute from within it and according to its language. This is how we must interpret the arrangement in section 3 of the Act because, as we previously held, so long as the potential infringement involved in the provision of the statute can be limited by interpretation, the interpretive move should be advanced, thereby exercising constitutional review according to the Limitations Clause (and see CrimA 6659/06, *John Doe v. State of Israel* (unpublished, June 11, 2008) hereinafter: "the Unlawful Combatants case", para 7).

As we know, the Court's interpretative work is done according to the limitations obliged by the language and purpose of the statute, in addition to presumptions of interpretation accepted in our legal system which the interpreter may utilize (the Unlawful Combatants case; HCJ 9098/01, *Genis v. Ministry of Construction and Housing*, IsrSC 59(4) 241 (2004) (hereinafter: "Genis"). As the point of departure in the work of interpretation the Court will, so far as possible, seek to avoid striking a

statute enacted by the Knesset in deference to the legislature and the separation of powers that stands at the centre of the Israeli legal system. The Court will therefore often prefer to leave the statute as it is, applying an interpretation that is adaptable it to the constitutional system and fundamental values. Accordingly, we shall seek to adopt an interpretation of the text that leads to the least infringement of human rights. As we said, for example, in the Unlawful Combatants case:

> "Our legal system presumes the legislature has knowledge of the contents and effects of the Basic Laws and every statute enacted after them. According to the presumption, a statutory provision is reviewed in an attempt to interpret it so as to befit the protection extended to human rights by the Basic Law. This achieves the presumption of normative harmony, according to which 'a discrepancy between legal norms is not presumed and every possible attempt is made to maintain 'legal uniformity' and harmony between various norms' (A. Barak, INTERPRETATION IN LAW – THE GENERAL DOCTRINE OF INTERPRETATION (1992), 155). … An effort of interpretation should be made in order, as much as possible, to reduce infringement on liberty so that it be proportional for the purpose of achieving security and no more. Such interpretation will be consistent with the basic philosophy prevailing in our legal system, that a statute ought to be implemented by interpretive means and as much as possible striking it down for unconstitutionality must be avoided" (*id*, para. 7).

And in HCJ 4562/92, *Zandberg v. The Broadcasting Authority*, IsrSC 50(2) 793, 812 (1996) President A. Barak stated**:**

> "It is better to achieve limits on a statute by interpretation rather than having to limit it by declaring part of the statute void for violating provisions of a Basic Law… A reasonable interpretation of a statute is preferable to finding it unconstitutional."

According to our said philosophy, based on the assumption that the legislature intends to limit infringement on human rights as much as possible, and especially the human rights enshrined in and protected by Basic Laws, there might be cases where, in order to achieve the purpose of the text and avoid striking it down, it is justified to interpret it more narrowly so that it will not apply, for example, to a particular category of circumstances.

President A. Barak's statement is apt here:

> "May the commentator limit the broad language of the text in order to achieve the purpose of the text? When the text prescribes a legal arrangement that applies to 'everyone' with respect to 'everything' in 'all circumstances', may the interpreter – who seeks to achieve the underlying purpose of the text – interpret the text so it does not apply to a particular category of persons (not 'every' one,) does not apply to a particular category of things (not 'every' thing,) and does not apply to a particular category of circumstances (not 'all' circumstances)? The

answer to this question in Israel and also in comparative law is in the affirmative. I considered this in the *Zandberg* case, stating: 'When the language of the statute is broad, the judge may and can give it a narrow meaning, extending to only some of the options emerging from the language, provided that he thereby achieves the purpose of the enactment. That is the case in Israel. That is the case in comparative law…

… Indeed, in order to achieve the underlying purpose of the statute – be it a specific or general purpose – the interpreter may give the broad language of the statute a narrow meaning" (Genis, p 37).

From the General to the Specific – the Interpretation of Section 3

16. Hence, it appears that under the circumstances here the petitioners' application can be considered in terms of interpretation, as a request for narrow interpretation that would limit investigatory authorities' ability to rely on general objectives for the purpose of orders to obtain communications data. To that end, we must, to use Justice M. Cheshin's metaphor, "peel the statute as one peels the integuments of an onion: healthy ones are kept and unhealthy ones discarded" (Genis, at 268). The "unhealthy integuments" are those cases where the investigatory authority might have applied to court for an order to obtain communications data for achieving general objectives. Although according to the language of the Law – and its language alone – there is no bar, on its face, to doing so, it does appear that in light of constitutional interpretation, consistent with the language and purpose of the Act, the investigatory authority is not authorized to act in that way and must apply for orders only in cases where the order is necessary for detecting a particular offender or for investigating or preventing a particular offense that is anticipated or being committed. This conclusion is consistent with the particular stated purpose of the Act, which concerns combating crime and the detecting and punishing of offenders, while limiting the use of the broad tool embodied in section 43 of the Criminal Procedure Ordinance. This conclusion is consistent with the general purpose of the Act, which calls for limiting the infringement on the constitutional right to privacy so that it is proportional in achieving the purpose of the Act (see also Genis, at 291-93, the Unlawful Combatants case, para. 8). This interpretation is consistent with the fundamental concepts of our legal system and brings about a proper balance between leaving the Act as it is and achieving the goals of Basic Law: Human Dignity and Liberty.

As mentioned, this is indeed the position of the State as well. In its notice of May 22, 2008 the State agreed to this narrow interpretation. According to the State, the language of the Act clearly indicates its drafters intended to permit issuing orders in order to obtain communications data only where necessary to inquire into a concrete suspicion rather than for gathering general intelligence. The State clarifies that, in its opinion, too, in requesting an order investigatory authorities must at least "indicate a clue, the first stage of a *prima facie* evidential foundation for police action relating to a concrete investigation," consistent with the relief the Association for Civil Rights seeks in its petition (para. 52 of the State's notice). Then chairman of the Knesset's

Constitution, Law and Justice Committee expressed a similar position (hereinafter: "the Constitution Committee") in the discussions around the Regulations for the Act's implementation. Thus, then chairman of the Constitution Committee, Prof. Menachem Ben Sasson, stated during the discussion held on August 13, 2008: "This Act must be elucidated narrowly. That is to say that where there is doubt, the answer is 'no'. I am not saying that as an interpreter of the Act but it cannot be interpreted otherwise and anyone participating in the discussions knows it…" (Transcript of meeting no. 639 of the Constitution, Law and Justice Committee of the 17th Knesset, 5 (August 13, 2008)). This limit on investigatory authorities' discretion, which is accepted by the State, also finds expression in the Police procedure that regulates Police action under the Act, which is none other than procedure 03.344.306 that was formulated after the Act came into effect and when the petitions were pending (hereinafter: "the procedure"). As for section 3, the procedure adds little to what the Act requires given the procedure in section 3 is very detailed. Thus, the procedure specifies, lifted directly from the Act's language, the details that any request for an order must included, as well as the considerations the officer seeking the order must apply. Those considerations are, *inter alia*, the severity of the offense and the strength of the suspicion, and the evidential foundation as to the request's subject matter. By following this, the Police activity in terms of these orders complies with the proper interpretation as established by us above.

It should be emphasized that our above interpretation of section 3 is not based on the State's concession as to the proper interpretation of the section or of other sections the petitioners have challenged. Nor is it based on the existence of the Police procedure. The State's concession or action may change as they are a product of the State's policy alone. Nevertheless, under the circumstances here, that concession also reflects the proper interpretation that, in our opinion, should guide how the authorities exercise their powers. This interpretation is consistent with the language of the text and its purpose (both particular and general), and it permits the arrangement prescribed in section 3 to subsist as a proportional arrangement that does not over-infringe the constitutional right to privacy. Indeed, it might perhaps have been preferable to amend the Act itself so that it embodies the approach – shared by the State, the petitioners and the Court – with regard to the narrow implementation of section 3's broad provisions. Nevertheless, interpretation is a tool at the Court's disposal and it enables us to clarify the boundaries of the Act, even if the actual language of the Act remains unchanged. We would go on to say that in the scope of our interpretive work of identifying the legislative intent we may be assisted by information the executive authority holds (see: Aharon Barak, INTERPRETATION IN LAW, PART TWO – LEGISLATIVE INTERPRETATION 346 (5753) (hereinafter: "Legislative Interpretation"). Thus, the procedure demonstrates the Act's legislative intent as viewed by the executive authority and that the interpretation it adopted is consistent with the interpretation that we have prescribed above. This joins with the other facts that have led us to conclude this is indeed the proper interpretation of the Act under review.

We have therefore reached the overall conclusion that the proper constitutional interpretation of sections 3(a)(2) and of 3(a)(3) of the Communications Data Act is that

investigatory authorities are empowered to request a court for an order under the Act only for the purpose of detecting concrete offenders or offenses rather than for general intelligence activity as to offenders or offenses. This interpretation achieves the second requirement of proportionality because, in our opinion, it constitutes a means that less restricts the right to privacy, while still achieving the purpose of the Act in the same way. This conclusion is also required by the State's concession to a narrow interpretation, which indicates that in its opinion the objectives for which the Act was passed will not be hindered by that narrow interpretation.

Given this interpretation, we have reached the overall conclusion that the arrangement in section 3 also meets the third requirement of proportionality because the extent of the infringement on the right to privacy – in the manner described – is in proper proportion to the benefit from applying the Act and its arrangements, a benefit which the petitioners themselves do not dispute.

17. A similar approach, that relates to the necessary balance between the right's infringement and the benefit to public interest characterizes parallel legislation in legal systems similar to ours, which have articulated various grounds for obtaining communications data – some more extensive than the grounds under Israeli law and some closer to the grounds included in it. Some countries have made the concrete nature of the offense or offender requirement clear as opposed to general aspects of law enforcement, and others have not. This reinforces our conclusion that in terms of the grounds for exercising authorities under the Act, and given the proper interpretation for their exercise, as delineated above, this aspect of the Israeli Act complies with the requirements of proportionality and is consistent with the constitutional concepts prevailing in legal systems that are similar to ours.

In English law, for example, the RIPA, mentioned above, regulates powers to obtain communications data in an arrangement that sets the various surveillance powers State authorities have, both to obtain the content of information and to obtain communications data without content. The Chapter that addresses the grounds for requesting communications data, regulated in section 22(2) of the RIPA, is relevant here. It details a very broad list of grounds for when communications data can be obtained. Not all the grounds make it possible to obtain all types of data and in any event obtaining them is subject to proportionality. The grounds are defined in the English Act as follows:

> "(a) in the interests of national security;
> (b) for the purpose of preventing or detecting crime or of preventing disorder;
> (c) in the interests of the economic well-being of the United Kingdom;
> (d) in the interests of public safety;
> (e) for the purpose of protecting public health;
> (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;

(g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health; or
(h) for any purpose (not falling within paragraphs (a) to (g)) which is specified for the purposes of this subsection by an order made by the Secretary of State".

From the above it is clear that the list of grounds in English law is far broader than those recognized in the Act subject to the petitions here. In American law as well, the accepted criterion for placing surveillance devices of the pen/trap device type – which require a judicial order – is relatively broad and examines whether the required data are "relevant to an ongoing criminal investigation" (18 USC §3123(a)(1) which is the ECPA, mentioned above). Reviewing section 2703(d), which addresses the conditions necessary for granting a judicial order to obtain communications data (which are similar to subscriber data and some of the traffic data in the Israeli Act), and also regulates the possibility of obtaining message content, a higher bar emerges, which is supplemented by the condition that the party requesting the order must indicate "specific and articulate facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation". On its face, the American standard does not limit the nature and gravity of the investigation but it does appear that, like in the Israeli Act as we described above, it is necessary that the information is sought for a concrete investigation. Canadian law, on the other hand, permits granting a judicial order when only two requirements are fulfilled – other means of investigation cannot be used (or they have been attempted and failed); and the order "would be in the best interests of the administration of justice" (see the Criminal Code of Canada, §186(1)(a)), namely in circumstances where granting the order will best serve justice.

Application of the Arrangement in Section 3 to Offenses of the Misdemeanor Type

18. As mentioned, the petitioners' second argument is that the Act as a whole – and section 3 in particular – should be applied to offenses that are defined by the Israeli Penal Law as "felonies" but not to those defined as "misdemeanors". As this argument goes, and reiterated in both petitions as well as in the position of the Press Council, offenses of the "misdemeanor" type extend over a wide range, a substantial proportion of which are not sufficiently serious to justify the infringing measures in the Act. Consequently, according to the argument, granting sweeping power in the Act to obtain a judicial order for all misdemeanors, without drawing lines based on the seriousness of the offense, is sweeping and not proportional. In support of this argument, the petitioners referred to the Secret Monitoring Act, which restricts the exercise of the power prescribed in it to felonies.

The State for its part does not believe that the petitioners' arguments in this regard justify amending the Act, let alone striking it down . In its introduction, the State explains that many misdemeanors are serious, very common offenses that affect the quality and integrity of life in the country. Thus, for example, the State mentioned

that these offenses include assault, fraud, forgery, breach of trust, computer hacking, sexual harassment, harassment by telecommunications device, obstruction of justice, witness harassment, giving information to the enemy, threats, negligent homicide and more. Serious misdemeanors are included in the Military Justice Act as well. The State therefore asserted that granting the relief sought and precluding investigatory authorities from obtaining communications data for misdemeanors would significantly impair their ability to perform their duties. Additionally, the State explained that there are misdemeanors that cannot be investigated without communications data, such as sexual harassment by a computer or telephone. The State also reiterated its position that the infringement caused by obtaining communications data is far reduced compared to that caused by other investigatory means, including secret monitoring. Therefore, according to the State, there is no justification for imposing a limitation based on the gravity of the offense, as prescribed in the Secret Monitoring Act. After all that, the State again emphasized that the Act prescribes many mechanisms intended to prevent its improper exercise, including for misdemeanors that do not justify it – from the detailed mechanism for submitting motions, through a court's role in authorizations, to the mechanism for reviewing the Act's implementation through reports to the Knesset and the Attorney General.

19. The Penal Law, 5737-1977 (hereinafter: "the Penal Law") prescribes in its definitions section that a misdemeanor is:

> "An offense punishable by no less than three months' imprisonment, but no more than three years imprisonment; and if the penalty is a fine – a fine higher than the fine that may be imposed for an offense punishable by fine the amount of which has not been determined ".

This definition applies to many of the offenses on the Israeli law books and it means that investigatory authorities' powers under the Communications Data Act cover a wide range of offenses, the severity of which varies. Consequently, the petitioners' argument that a sweeping application of section 3, without requiring authorities to consider the gravity of the offense, could indicate a disproportionate infringement on the right to privacy is understandable. In view of this, we somewhat hesitated as to whether it is indeed justified to leave misdemeanors to the sweeping application of section 3 or whether in this case as well the section should be narrowly interpreted so that only when particularly serious misdemeanors are concerned or where communications data is an inherent element of the offense (for example computer hacking) will it be possible to request the court for such an order.

Ultimately, we reached the overall conclusion that this aspect does not warrant our intervention and that this arrangement meets the requirements of proportionality. To be specific, regarding the first requirement of proportionality, there is no question that there is a rational relationship between the means and the end because including misdemeanors would significantly help the Police achieve legislative intent and it would appear that their blanket removal would likely impair that ability. Nevertheless, as mentioned, here again the second requirement of proportionality raises difficulties

because on its face, limiting the types of misdemeanor to which the arrangement applies similarly achieves the end but nevertheless reduces the infringement on the right to privacy. The position of the State in this respect is based on the nature of requests under section 3. According to the State, there is no justification for making a formal distinction between different types of misdemeanors for the purpose of applying the Act and the focus should be on the need for the request. To that end, according to the State, the Act establishes balances and checks that do not consider obtaining communications data as trivial but present a detailed mechanism for submitting the request. Moreover, as mentioned, these requests are submitted merely for the court's approval and the court must review all the relevant aspects, including whether obtaining the data in order to detect the concrete offense infringes the right to privacy beyond that necessary. Again, the array of reports to the Knesset and the Attorney General should ensure that the arrangement is only used when appropriate.

Under the circumstances, it appears to us that the mechanisms in the Act – and especially the motion's judicial review – may certainly provide at this time an adequate resolution for the petitioners' concern as to the arrangement's improper use. It should be added that according to the reports that were submitted to the Knesset in 2009 and 2010 as to the implementation, 60% to 70% of the motions for a judicial order were made and approved regarding felonies. As regards misdemeanors for which a judicial order was sought, it appears that between July 2009 and June 2010, a substantial proportion of the offenses would apparently have been considered by the petitioners, too, as "serious offenses", including threats, theft, negligent homicide, harassment, arson, killing, vandalism, causing damage and more. These data indicate, on their face, that in the implementation of section 3 in terms of misdemeanors is not treated lightly and the data above certainly do not demonstrate the alleged disproportionality resulting from including misdemeanors under the section. Under the circumstances, and considering the restraint that we exercise in intervening in legislation, we have not found it justified for us to intervene in this determination by the legislature. Nevertheless, there is no doubt that the courts that grant the various motions are tasked with considerable work – to ensure the Communications Data Act is used solely in the cases where it is necessary according to the interpretation adopted above. In this respect it is clear that courts would have to analyze whether the nature of the offenses for which the orders are sought necessitate exercising the powers granted by the Act in light of the privacy infringements they cause. Courts would also have to consider the possibility that the extent of infringement by one type of data might be greater than another.

Apt in this respect is the Canadian Supreme Court's ruling in *R. v. Araujo* [2000] 2 SCR 992, Par. 29, which our courts should also apply as a point of departure when considering various different motions to obtain data under the Act:

> "The authorizing judge stands as the guardian of the law and of the constitutional principles protecting privacy interests.

> The judge should not view himself or herself as a mere rubber stamp… The authorizing judge should grant the authorization only as far as need is demonstrated by the material submitted by the applicant. The judge should remember that the citizens of his country must be protected against unwanted fishing expeditions by the state and its law enforcement agencies."

As stated there, judges are duty-bound to safeguard the Act and the protection of privacy, and they must bear in mind that the State's citizens should be protected against a fishing expedition conducted by law enforcement agencies.

Assuming that this power will be exercised only when appropriate, we believe that the arrangement that covers misdemeanours also meets the third criterion of proportionality because the infringement to privacy caused by its application is in proper proportion to the benefit from exercising the authorities the Acts grants.

20. It appears, regarding the types of offense that justify obtaining communications data, different legal systems have adopted different arrangements that are essentially based on the same principles. Thus, for example, it seems the American legislature did not see fit to limit the power to obtain data along the "ordinary" track – by judicial order under chapter 18 of the USC – to a particular type of offense. In English law, too, there is no such restriction and the grounds permitting obtaining communications data are, as mentioned, broader. It should nevertheless be noted that English law does define "serious crime", but solely in the context of obtaining content data. According to the definition, a serious crime is one that carries, for an adult without relevant previous convictions, an expected sentence of at least three years imprisonment. It is also a crime committed in collusion, a crime committed with the use of violence or a crime leading to substantial financial gain. Hence, it appears that the English legislature also prescribed a threshold for the definition of a "serious crime" that does not make do with defining the offense according to the likely penalty for it, but also takes into account the circumstances in which it is committed. This substantive view with regard to the offense and its gravity is similar to the State of Israel's position regarding cases in which it could be appropriate to act according to the arrangement in section 3. On the other hand, Canadian law, which regulates the issue through the Canadian Criminal Code, details a very extensive list of various offenses defined as serious. The Canadian list includes more than 100 offenses (see section 183 of the Criminal Code). Hence, we again see that different countries have prescribed different arrangements as to the types of offenses resulted in requests for obtaining communications data. We can infer from this that it is at least possible to articulate several means that achieve the purpose in the same way and it clearly cannot be said that the Israeli arrangement goes beyond those applied in countries with a similar constitutional regime. The arrangement therefore does not exceed the bounds of proportionality so that they justify the Court's intervention.

21. Consequently, regarding section 3, we have reached the overall conclusion that subject to our interpretation of above observations, the arrangement in section 3 meets

the requirement of proportionality and we have therefore not found there is constitutional grounds for our intervention.

Section 4 – Administrative Order

22. Section 4 of the Act prescribes a different arrangement that does not condition obtaining communications data upon a judicial order. Instead it allows investigatory authorities to obtain communications data in urgent cases through an order from a professional entity (hereinafter: "the administrative arrangement"). The language of the section is as follows:

> *"Permit to Obtain Communications Data in Urgent Cases*
>
> 4. (a) A competent officer may – at the request of a policeman or military policeman, as the case may be – grant a permit to obtain communications data from a telecommunications licensee's database without a court order under section 3, if he is satisfied that, in order to prevent an offense that is a felony, to detect its perpetrator or to save human life, it is necessary to obtain the said communications data without delay and that an order under section 3 cannot be obtained in time."

According to the petitioners, the arrangement in section 4 is disproportionate because it permits an administrative – rather than judicial – entity to issue an order that enables a serious infringement of privacy without the restrictions imposed on courts by section 3, especially in terms of professionals. The petitioners, who are also joined by the Press Council in this respect, focus their arguments on the following two. Their first argument is that the investigatory authorities' power to obtain the communications data of professionals, especially journalists and attorneys, by administrative order is not proportionate. This is essentially because that power is not subject to restrictions similar to those the Act imposes on communications data orders regarding professionals because section 4 – unlike section 3 – does not refer at all to the aspects relating to obtaining an order in urgent cases when professionals are involved. According to the argument, enabling an administrative entity to infringe legal privilege without a judicial order is not proportionate. These arguments were presented to us by the entities that represent such professionals. As metioned, the Israel Bar filed a petition addressing the alleged damage to lawyers' occupation because this compromises attorney-client privilege. The Press Council joined the general petition as amicus curiae and presented its arguments as to the likely damage to journalists' occupation caused by section 4, in light of the potential exposure of journalists' sources. The Press Council applied to the Court for the principal relief of an order striking down section 4 in terms of journalists so that a motion for obtaining communications data of journalists would be only allowed under the mechanism set in section 3(b) of the Act, namely by a judicial order alone, and only if there are grounds to suspect the journalist is involved in an offense. The other argument against the arrangement in section 4 made during the hearing concerned the method of

implementing the arrangement and its alleged excessive use. In this context it was also argued that judicial and administrative review of investigatory authorities' exercise of their powers under the arrangement is deficient.

23. The State asserted in response that the benefit of this arrangement exceeds the infringement of the right to privacy caused by obtaining communications data urgently without a judicial order. According to the State, the need to save lives or immediately detect offenders at the crime scene does, in urgent cases, justify forgoing judicial review facilitated by a court procedure as provided in section 3 addressing the population as a whole, without having to make a specific distinction in the case of professionals. As appears from the State's reply "the urgent cases which section 4 addresses are extreme… in cases of saving life, in urgent cases of solving a crime when the professional is the victim of a felony or is missing and must be found urgently, where it is necessary to obtain the professional's communications data in order to prevent a felony of which he is suspected and other urgent cases of similar nature" (see para. 61 of the State's reply of May 22, 2008). Moreover, the State asserted that the urgent arrangement is applied sparingly and limitedly according to relevant Police procedures. As discussed, on February 16, 2009 the State furnished for our review the Police procedure that regulates the Act's application, formulated after the Act came into effect. The procedure is based on section 4(f) of the Act, which provides that "the Inspector General … shall ... prescribe provisions for the purpose of this section, including how the permit is granted … and may prescribe different provisions according to the grounds for granting the permit and the circumstances in which it is granted." The procedure emphasizes and clarifies the Act and limits the competent officer's discretion in two significant respects. Thus, in terms of the factors the competent officer must consider before authorizing obtaining communications data without a judicial order, the procedure replicates the factors the officer must consider before applying for a judicial order. It then adds other factors as to the existence of an urgent need to prevent an offense, to detect its perpetrator, or to save human life. These factors also include the type of communications data sought, the severity of the offense and the extent of the damage to those who are not suspects.

As to professionals, the procedure distinguishes between journalists and others referenced in the procedure: lawyers, doctors, social workers, clergymen, psychologists, government ministers and Knesset member. In regard to urgently obtaining professionals' communications data, the procedure mandates that: "if the subscriber is a professional, that should be specifically taken into account and the necessary balance should be made between the possibility of infringing the professional's privilege and the benefit that the communications data might have in the specific investigation, factoring in the seriousness of the offense, the circumstances of its commission, the likelihood the communications data will indeed lead to discovering the truth and detecting the offenders" (para. 7B(4) of the procedure). Regarding journalists the procedure lays down a narrower arrangement, providing that "insofar as it is known that the subscriber is a journalist, who is neither suspected of the offense nor the victim, the competent officer shall not authorize obtaining their communications data or the traffic data type (a list of incoming and outgoing calls)."

This distinction is *inter alia* based on the State's position, as detailed above, according to which, but for journalists, in the absence of power to obtain the content of calls the Communications Data Act does not infringe the various different professional privileges. Nevertheless, the State agrees the different privileges in the context of making a decision to grant an administrative order must be considered, and this is within the competent officer's discretion. According to this set of balances, the State believes that under the circumstances the arrangement is proper and proportional.

(a) *Is the Arrangement Prescribed in Section 4 Proportional?*

24. On the face of it, it is clear that the arrangement in section 4 is narrower than that prescribed in section 3. Thus, it applies only to offenses of the felony type and it is plain from its wording – and the State also elucidated the same in its reply – that it applies in concrete cases in which there is an urgent need to prevent an offense, detect a perpetrator or save human life. Our interpretive finding, that the provisions of the Act do not grant power to obtain an order in circumstances where the order is sought for general intelligence activity detecting offenses, therefore also applies to section 4. That is indeed the proper interpretation of the section. Moreover, section 4 permits only the Police or the Military Police CID, and no other investigatory authorities, to obtain communications data urgently, and it is effective only for 24 hours.

Nevertheless, the arrangement extends the power of investigatory authorities to obtain communications data without a judicial order. Thus, for example, until the Act became effective, the investigatory authorities followed the Attorney General's Directive 4.210 (90.013) (The Delivery of Information by Telephone Companies to Entities Having Investigatory Authority), which provides that without a judicial order communications data (other than the name, address or telephone number of the subscriber) cannot be obtained, unless the defense of necessity applies in the particular case. This threshold, which required immediate, urgent danger that justifies obtaining communications data, has been lowered in the current arrangement. Moreover, the arrangement lacks section 3's restrictions to discretion, particularly the restriction on transferring professionals' communications data. According to this arrangement, as set in the Act, it is *prima facie* possible to transfer a professional's communications data without any restriction when authorized by a competent officer, who is satisfied there is an urgent need to do so. These restrictions, albeit not in full, do appear in the Police procedure that regulates both the competent officer's discretion to authorize administrative permits and the obtaining of professionals' communications data.

The petitioners' arguments in this context reflect both aspects. The first aspect is at the level of the administrative discretion. In this respect the petitioners argued that restrictions in addition to those specifically mentioned in section 4 should be imposed on how the administrative discretion is exercised. The other aspect, according to the argument, concerns the Act's actual infringement on the various different privileges.

25. The point of departure necessary for reviewing the proportionality of the arrangement is based on our above finding that, in general – apart from in the case of

journalists – the Communications Data Act does not infringe the various different professional privileges. This is considering the scope and extent of those privileges as recognized by Israeli law, compared to the data that can be obtained by applying the Act's arrangements. In the absence of such infringement, *prima facie* it cannot be said that because section 4 does not refer to professionals *per se* it must be struck down for unconstitutionality. This is reinforced especially because the purposes of sections 3 and 4 are not the same. While section 3 is intended to enable obtaining communications data in the cases detailed in the section, which by their nature give the authorities adequate time to turn to a court, section 4 is designed to give the Israel Police and the Military Police CID a tool for cases where there is an urgent need, that cannot be delayed, to obtain the data without approaching a court. This distinction between the purpose of the sections can on its face also justify a distinction regarding professionals so that where there is urgent need, for example in life-threatening cases or because of the gravity of the matter, the weight attributed to protecting their privacy would be diminished. For such cases, it is difficult to say that the mere absence of an express provision of the Act relating to professionals amounts to a constitutional flaw that justifies our intervention.

26. Nevertheless, despite the arrangements' different purposes, we cannot help but wonder why the legislature saw fit to set out such a detailed arrangement in section 3, which delineates how the discretion of administrative authorities and courts dealing with applications to obtain data must be exercised, while in section 4, which concerns only how administrative authorities' discretion must be exercised, there is no similar detail whatsoever. We have not been satisfied, nor has it been pleaded to us, that there is any particular difficulty in establishing more detailed guiding criteria in section 4 as well, to give proper weight to its different purpose. Thus, for example, in the case of professionals, section 3 provides that "the court shall not permit obtaining communications data… unless it is satisfied, on the basis of clear details to such effect in the motion, that there are grounds to suspect that the professional is involved in the offense for which the motion was filed." As aforesaid, in view of the difference between the arrangements, we have not found that the legislature was required to prescribe identical arrangements. Nevertheless, along the lines of the legislature's provision in section 3, it would be proper, while exercising power section 4 of the Act grants, that the authority considered that the subscriber is a professional and decides whether it is appropriate to obtain communications data in such case considering the proper balance between the privacy infringement and the urgent need to obtain the data. The considerations should also include the reservations required by the fact that the details sought involve professionals who have a special interest in not disclosing the data. In this context the authority clearly could also consider whether it is appropriate to order obtaining communications data even where the professional is not involved in the offense.

The Act's language certainly does not limit such an interpretation regarding how the power granted by section 4 of the Act must be exercised. It is also consistent with the particular purpose of the arrangement because it does not preclude the issue of an appropriate order in urgent situations in terms of anyone, depending on the competent

authority's needs. It is also such as to create internal harmony between the Act's sections by attaching greater weight to the duty to consider the right to privacy when professionals are involved, along the lines of the legislature's own determination in section 3. In addition, this interpretation achieves the general legislative intent because it gives greater weight to the constitutional right to privacy. This interpretation thereby constitutes the least restrictive means, while achieving the arrangement's legislative intent in a similar way. Consequently, it appears to us that this interpretation is the proper one regarding how the authority should exercise its power under section 4.

It should be noted that this is in fact apt not only as to professionals, but also as to the overall aspects emerging from section 3 and the restrictions on judicial discretion that the legislature mandated in it and which should of course also guide the administrative authority when exercising its power under the arrangement in section 4. In fact, the restrictions section 3 imposes can be viewed as part of the overall relevant considerations that must come into account when exercising the powers granted by the Act, in light of the arrangements' different purposes. This aspect in fact mirrors the axiom of administrative law that an authority must exercise its power while weighing all relevant factors and ignore improper factors (Daphne Barak-Erez, *Administrative Law* vol. II 642 (5770); HCJ 953/87, *Poraz v. Shlomo Lahat, Mayor of Tel Aviv – Jaffa*, IsrSC 42(2) 309, 324 (1988)). Thus, for example, alongside the special reference to professionals that we have discussed at length, it appears that before deciding to permit obtaining communications data, the type of communications data sought, the extent of the infringement to anyone not suspected, the gravity of the offense, the urgency and the ability to take the judicial track under section 3, and which option should be given first preference are, among others, the factors to be considered. Let there be no doubt that in light of the differences in circumstances around implementing the arrangements, the authority need not attribute similar weight to each of these considerations, and the decision should be made in light of the particular circumstances of the case. Nevertheless, it does appear exercising the power under section 4 is subject to particularly strict review of all the above factors.

27. It appears the State, too, accepts this approach as to how the power under section 4 must be exercised in terms of professionals – and generally. Thus, it asserts in its reply that the administrative arrangement in section 4 was essentially designed to be used in extreme cases where the professional is the victim of an offense or suspected of a felony, or in extreme cases of saving life. Given that, it appears that the State also believes that the difference between the restrictions imposed by the arrangement in section 3 and those imposed on the party seeking to obtain data under section 4 is not so great. Bear in mind that the petitioners' basic argument is that section 4 is disproportional because it does not prescribe conditions similar to those in section 3 of the Act. Consequently, given to the proper interpretation which requires exercising discretion in a way that considers all the factors necessitating obtaining communications data, and in light of the State's position as to how that principle should apply, it appears the argument regarding section 4's disproportionality fails.

As discussed, the administrative arrangement's purpose – saving human life, preventing serious crimes of the felony type or quickly detecting an offender who has committed a felony – is achieved through this tool, which prevents having to approach a court and awaiting a judicial order. This tool is of course restricted and clearly should only be used where "the main road" – seeking a judicial order under section 3 – cannot be followed. Thus it appears there is a rational connection between the means and the end and that the arrangement would only be implemented where the end cannot be achieved by other means. This is where the very court proceeding makes the Police unable to obtain communications data "in real time", in very urgent cases that necessitate doing so. Even when approaching a court can be done as quickly as possible, the same speed as when a competent officer who is always accessible and whose authority to obtain communications data immediate, is impossible. The State's examples as to the cases where this procedure is used demonstrate this. At the same time, it also appears the Police acknowledges the potential privacy infringement the administrative procedure causes and the proper interpretation as to the exercise of the power as found here, which also appears to be accepted by the State, therefore further limiting the competent officer's discretion. These restrictions, and paying strict attention to applying the administrative process only in serious, urgent cases, in our opinion reflects a proper balance between infringing the right to privacy and the need for Police immediate action.

This approach as to how the power granted by section 4 should be exercised is also reflected in the Police procedure, which, according to the Police, achieves the proper balance between infringing privacy and the purpose of obtaining the order under section 4. Regarding professionals, and how we believe the power must be exercised, the procedure emphasizes the importance of safeguarding their privacy and the privacy of their clients, and it requires the competent officer to carefully examine the need for administrative order, considering the gravity of the offense, the circumstances of its commission, and the likelihood that communications data would indeed result in detecting the truth and discovering offenders. Nevertheless, the procedure does not apply all the restrictions prescribed in section 3 and does not limit the use of administrative order for professionals solely to cases where they are involved in an offense – except in the case of journalists. As mentioned, in our opinion, the purpose of the arrangement in section 4 is not the same as that of section 3 and the arrangements therefore need not be identical. This difference is, as noted, found in how some aspects of section 4 are narrow compared to section 3. As mentioned, including restrictions in the procedure does not demonstrate their proper interpretation as to the exercise of the power in section 4. However, the procedure does express the authority's position in this respect and this is coupled with the overall factors leading to the conclusion that our above interpretation is the proper one.

In light of all the above and the legislative intent behind section 4, recognizing the importance of cases where an urgent need can justify infringing professional privilege, and considering the limited infringement of privilege obtaining the data that the Act permits causes in any event, it appears to us that the arrangement in section 4, as written, given its proper interpretation, which requires considering the issue of

professional privilege and other aspects as mentioned, does not require additional legislative restriction over the authority's power in this context. This arrangement, which appears in the Police procedure too, therefore expresses in our opinion the proper equilibrium between protecting the right to privacy and the sometimes urgent need to obtain communications data, and as such we have found that it meets the criteria of proportionality.

28. As we have mentioned above, and as noted that the State agrees with this approach, different treatment of the journalist's privilege is appropriate. The State was therefore correct in prescribing special conditions for journalists in the procedure. As mentioned, according to the procedure, if the subscriber is a journalist who is neither suspected nor the victim of the offense, the competent officer will not authorize obtaining communications data of the traffic data type. In this way the journalist's privilege has special protection in the procedure. Nevertheless, in cases in which the journalist's life is at risk or in which the journalist is himself suspected of offenses – and it should be borne in mind that only offenses of the felony type are relevant – and in exceptional circumstances when because of their urgency it is impossible to approach a court to obtain a judicial order, it is indeed appropriate to permit obtaining a journalist's communications data, even if this might be at the cost of infringing a source's privilege. In such circumstances we do not believe there is any foundation to the argument that infringing the journalist's privilege is disproportional. Here again it should be borne in mind that the procedure reflects how the authority interprets the Act in terms of journalists. As said above, through our interpretive work, the interpreter may refer – amongst the other sources available to him in understanding the legislative intent and its proper interpretation – to the information in the possession of the executive authority, as revealed by its secondary legislation (see Legislative Interpretation 346, 800-802). This information does not of course obligate the court insofar that it believes there is a more proper interpretation for the statute. But it can help in making the interpretation and ascertaining the purpose of the legislation (see HCJ 142/89, *Tnuat Laor v. The Chairman of the Knesset*, IsrSC 44(3) 529, 550 (1990)). In the instant case it appears that although there is no relevant secondary legislation and the procedure has inferior normative standing, the procedure indicates that the executive sees the purpose of the Act and the interpretation it adopted for it is consistent with the interpretation we stated above. In the circumstances, it appears the proper interpretation is the one the State follows and thus, too, it ought to be adopted.

29. To complete the picture, we would mention that English law has an arrangement similar to that emerging from the Israeli procedure. There, the different treatment of professionals in gathering communications data is also regulated in a procedure, rather than a statute (Interception of Communications: Code of Practice (London, 2002)). There, too, sections 3.2 and 3.9 of the procedure provide that when permitting access to the communications data of anyone not directly linked to the data sought, the utmost care must be taken, especially where the information infringes legally recognized privilege or the data is personal, which by its nature is generally kept private or confidential. Section 3.2 of the procedure provides as follows:

"Confidential Information

3.2 Particular consideration should also be given in cases where the subject of the interception might reasonably assume a high degree of privacy, or where confidential information is involved. Confidential information consists of matters subject to legal privilege, confidential personal information or confidential journalistic material…

For example, extra consideration should be given where interception might involve communications between a minister of religion and an individual relating to the latter's spiritual welfare, or where matters of medical or journalistic confidentiality or legal privilege may be involved".

Nevertheless, the statute and procedure there do not prohibit transferring data despite these privileges (even for journalistic privilege). Transferring such data is subject to the doctrine of proportionality, which as an overarching principle covers all the arrangements in the statute (see section 5 of the procedure). In this respect it should be noted that the English procedure was approved by Parliament. Again, Canadian law, in which the treatment of communications data is regulated by the Criminal Code, permits access to the communications data of practicing lawyers through a judicial order but only in circumstances where the lawyer himself is involved in the investigated offense or is likely to be its victim (section 186 of the Canadian Criminal Code). The Canadian arrangement is thereby similar to that prescribed in section 3 of the Israeli Law and also to a large extent, as in the interpretation adopted by us, to the way in which the arrangement in section 4 is applied to professionals.

30. As mentioned, we were not originally satisfied in light of the specific purpose of section 4 and the limited potential infringement of privilege of most professionals caused by obtaining the data the Act permits, the section's lack of specific reference to professionals does not indicate a lack of proportionality. *A fortiori* the same is the case in view of the section's proper interpretation as to cases where section 4, whose arrangement is also acceptable to the State, should be applied. As noted, we have looked at journalists somewhat differently but it does appear the special treatment to the procedure affords journalists does in fact express the proper interpretation of section 4 in their regard. In view of all this, we have reached the overall conclusion that the arrangement is proportional and properly balances the purposes of the Act and the infringement to the right to privacy. Here again, like our process of interpreting section 3, we view the Police procedure and the restrictions imposed by it as reflecting the Act's proper interpretation. This interpretation is consistent, as said, with the Act's language and achieves its purposes. This interpretation is also consistent with the basic concepts of our legal system and our duty to exercise judicial restraint in intervening in the Knesset's legislation. We have therefore considered it proper to adopt it (compare: HCJ 1911/03, *The Association for Civil Rights v. The Minister of Finance*, (unpublished, November 12, 2003)).

We would mention that we have not ignored the petitioners' claim that the State could change the procedure or even revoke it completely. We have also considered the petitioners' assertion that the procedure cannot "cure" a constitutional flaw in the Act, insofar as such flaw exists. Nevertheless, in view of our finding that section 4's proper interpretation and its detailed reflection in the procedure the State presented, we do not believe that there is cause for us to intervene in the statutory arrangement as it is written. Naturally, a change in the authority's conduct could also lead to a material change in the balance embodied in the Act. Such a change would give rise to new cause to challenge the Act, certainly at the administrative level and perhaps even the constitutional level. However we must not get ahead of ourselves and we can only assume that the administrative arrangement will be implemented according to the proper interpretation – sparingly, in extreme cases, for the purpose of dealing with offenses that necessitate so and only where urgency makes it clear that it would be impossible to obtain a court order under section 3. This is when the reasons for not approaching a court are circumstances relating to saving life or other serious circumstances, all considering a variety of factors, including the fact that the subscriber is a professional, the extent of his involvement in the offense, and the type of data sought, etc.

It should nevertheless be noted, to complete the picture, that the other legally empowered authorities have not produced procedures to us that are similar to the Police procedure concerning the way they exercise these powers. The Military Police CID has a duty to prescribe such procedures under section 4(f) of the Act. In light of our findings as to the proper interpretation of how the Act's powers must be exercised, and its compliance with the principles delineated in the Police procedure, we assume that the other authorities that operate under the Act will not exercise their statutory powers without applying similar criteria for exercising the authorities in the Act and formulating appropriate criteria to regulate those aspects.

(b) *The Act's Practical Application*

31. In the time when the petitions were pending, the petitioners added to their case another claim essentially concerning the implementation of the Act in the years before it came into effect. At the heart of this argument was the petitioners' concern that the investigatory authorities would exploit the powers granted by the Act where they could employ other less restrictive means. To support these arguments, the petitioners analyzed the data produced by the State about the extent of the Act's use, which according to them demonstrate that the powers the Act has granted hare overused. Although the petitioners sought to establish constitutional cause to strike down the Act, it appears the argument is ultimately on an administrative law level, and challenges upon whom powers conferred by the Act are exercised. The petitioners therefore sought to show a flaw in the authorities' discretion in implementing the Act or at least to express concern in how the discretion will in the future be exercised.

32. From the material before us, it does indeed appear the petitioners are not the only ones concerned about the extent to which the powers the Act grants are exercised.

The Constitutional Committee, which debated a motion to approve regulations of the database under section 6 of the Act, also expressed similar concern to the Police. This emerges, for example, from studying the transcripts of the proceedings of the Constitution, Law and Justice Committee dated August 13 and November 9, 2008, during which then chair of the Committee, Professor Menachem Ben Sasson, expressed his opinion that the Act should be interpreted narrowly. Concern was also expressed that the Police might use its powers under the Act excessively. The Constitution Committee of the current Knesset, headed by MK David Rotem, which met on February 2, 2010 in order to follow up the Act's implementation, also emphasized the importance of correctly and cautiously using the tools the Act provides.

The petitioners, for their part, used the concerns the Constitution Committee expressed on August 13, 2008 to support their position on the use of the Act's powers and asserted these concerns demonstrate that the Israel Police contravened Act's provisions. The State, in its replies, explained that the concerns raised in the Constitution Committee's 2008 debates were essentially about mishaps resulting from the fact that the Act's implementation was in its early days. Additionally, the State strongly rejected the petitioners' arguments that the Police contravened the Act's provisions.

As to the actual use figures, the State presented us with very little data, which related solely to the use of section 4 of the Act (an administrative order) from its effect date (in June 2008) until the end of 2008. Those data shows that a total of 546 permits were sought in cases of life-saving, 85 in the prevention of future felonies and 124 permits were to detect perpetrators of felonies that had already been committed.

Nevertheless, studying the Constitution Committee's portal on the Knesset website shows that to date various authorities have submitted two annual reports to the Committee according to the Act (available at http://www.knesset.gov.il/huka/FollowUpLaw_2.asp). The first report, filed by the Israel Police, is relevant to the period between June 27, 2008 and June 30, 2009. This report shows that 9,603 motions were filed and granted under section 3 of the Act (a judicial order). Of them, 9,227 were motions for detection and investigation of offenders, 252 were for saving of human life, and 124 were for seizure of property. The breakdown between felonies and misdemeanors is unclear. Nevertheless, a supplement submitted to the chair of the Constitution Committee on February 1, 2010, shows that as in 2009, more than 60% of the total offenses for which an order was sought were felonies. On the other hand, the Police's second report, which was relevant to the period between July 1, 2009 and June 30, 2010, reveals that 14,133 motions were filed under section 3, namely an increase of about 4,500 (or approximately 50%). Of the motions filed in that period, 13,946 were for the purpose of detecting offenders and investigating offenses, 185 for the purpose of saving human life and two for seizure of property. Of the total offenses for which the order was sought, 71% were felonies.

According to section 4 the Act (an administrative order) the first report reflects that 2,031 urgent permits were sought. 1,513 were for the purpose of saving human life

and 518 for the purpose of preventing a felony and detecting the perpetrator of an offense. The second report reflects that under this section 3,039 applications were made, namely an increase of about 1,000 (a rise of approximately 50%). 2,192 were for saving human life and 847 were for preventing a felony and detecting a perpetrator. Data were not produced as to the orders sought for professionals. Hence, it appears that there was a significant increase in the Israel Police's use of the Act.

As regards the Military Police CID, The first report indicates that between November 1, 2008 and November 3, 2009, 1,381 motions for orders in under section 3 were filed, the majority for detecting and preventing offenses, conducting investigations, detecting offenders and their prosecution. The second report that was furnished by the Military Police CID relates to a shorter period from January 1, 2010 to July 1, 2010, and it indicates that 703 motions were filed to obtain orders under section 3. These included 38 motions for the purpose of saving or protecting human life, 340 for detecting, investigating or preventing offenses, 325 for detecting and prosecuting offenders and none for seizing property. It appears that on average there was no change in the total motions the Military Police CID filed under section 3.

In respect to motions under section 4, it seems that on average there was some increase in their number. While the first report states that 58 administrative requests were approved, including 6 cases for urgent policing, 4 cases for urgent investigatory purposes to prevent a crime and in 48 cases for the purpose of saving human life, the second report (relating, as mentioned, to only seven months) stated that 44 requests were filed, in six cases for urgent investigatory purposes to prevent an offense, 37 cases for saving human life and 1 for urgent policing purposes.

Reports were also received from the other authorities granted powers under section 3 of the Act. The data of the Tax Authority shows that between July 2008 and July 2009, 146 motions were filed under section 3, of which 145 were approved. Between July 2009 and June 2010 the number of motions doubled to 318. The Police Internal Investigations Department filed 388 motions between June 2008 and June 2009. The Police Internal Investigations Department filed 406 motions between June 1, 2009 and May 31, 2010. 44% of the motions were for felonies and 56% related to misdemeanors. The Antitrust Authority filed motions for 4 orders in the period between June 27, 2008 and June 16, 2010. Until June 2009 the Securities Authority obtained 13 orders; between July 2009 and June 2010 it obtained 12 orders, including 3 relating to people with professional privilege. Between June 2010 and June 2011, 19 orders were issued, including 2 relating to people with professional privilege.

33. All the above figures reveal only a partial picture. On the one hand, it appears, *prima facie*, that some authorities, especially the Israel Police, have significantly increased their use of their powers under the Law – both section 3 and section 4. On the other hand, we have no explanation as to the change in the total use of the Act's powers, which could actually be justified. In any event, in the current circumstances we do not see it necessary to review these aspects further. This is first because in practice all the petitioners' arguments in this respect concern aspects of the Act's

implementation which do not, certainly not directly, go to the matter of its constitutionality. We have indeed already held in several contexts that implementing an administrative act can raise the question of its proportionality (HCJ 9593/84, *Rashad Murad v. The Commander of the IDF Forces in Judaea and Samaria* (unpublished, June 26, 2006); HCJ 9961/03, *The Centre for the Protection of the Individual Founded by Dr. Lotte Salzberger v. The Government of Israel* (unpublished, April 5, 2011)). We have also held that the implementation of a statute can impact its meeting the proportionality criteria (HCJ 6427/02, *The Movement for Quality Government in Israel v. The Knesset* IsrSC 61(1) 619 (2006), HCJ 6298/07, *Yehuda Ressler v. The Israel Knesset* (unpublished, February 21, 2012) paras. 19-22 of my opinion). Nevertheless, it appears that at the moment no justification has yet emerged for our intervention in this context. This is essentially based on the fact that the statute charges the Attorney General and the Israel Knesset with the task of reviewing the Act's implementation. Their work in this respect is merely beginning. Nevertheless, from the material presented to us and the Israel Knesset's position as reflected in its arguments, it appears on its face that the Knesset is acting according to its duties, and that it is aware of the concern of excessive use of, or extending, the powers under the Act to improper cases. Therefore we believe that for the time being various authorities should be permitted to do their work with the tools at their disposal. This should be coupled with the fact that our findings and the proper interpretation for the Act's implementation would certainly help to maintain the proportionality of the authorities' action under the Act and thus, too, all the authorities – both those that operate under the Act and those responsible for reviewing its implementation – should be permitted to create an accepted best practice routine according to the boundaries and restrictions we outlined. Under these circumstances, at the moment it is inappropriate for us to intervene in the aspects of the Act's implementation. Hopefully there will be no need for us to consider them in the future either. Nonetheless, we have not overlooked the fact that the duty to report to the Knesset as prescribed in the Act was established as a temporary provision that is in effect only for four years from the date the Act took effect (see section 14(c) of the Act). It appears to us that because of the difficulties associated with the Act's growing pains, which even the State does not dispute, the period of time necessary for assimilating the principles binding the authorities and the importance we attributed to the Knesset's consistent review, it is appropriate to take action in order to extend the effect of that section. It could even be made permanent. We would also reiterate that it should not be ignored that aspects of a statute's implementation might also affect review of its proportionality, and that the concern that the tools the Act granted be used excessively, especially given the significant increase in the number of motions filed, is real. Consequently, if in the future there is a change in the balance between the Act's use, we do not discount the possibility the petitioners or others would once more be able to approach the Court for relief.

Sections 6 and 7; the Database

34. Another argument by the petitioners challenges the arrangement in sections 6 and 7 of the Act, which establishes a database to be kept by the investigatory authorities (hereinafter: "the database"). These sections provide as follows:

"Requirement to Transfer an Information File from the Database of a Telecommunications Licensee

6. (a) The head of the Investigations and Intelligence Division may require a telecommunications license holder providing domestic landlines or mobile radio telephone services to transmit to him by computerized methods an up-to-date information file, as specified in paragraphs (1) and (2) below, which is in the licensee's database:

(1) Its subscriber's identifying details, as well as the identifying numbers of his telephone devices or of any components thereof;

(2) Information on the map of antennas which the licensee uses to provide telecommunication services by mobile radio telephone, including identifying data of each antenna and the areas it covers.

Keeping Information Files in a Protected Database

7. (a) An information file transferred as provided in section 6 shall be kept by the Police in a confidential database (to in this Act referred as 'database of (communications) identification data').

(b) The database of (communications) identification data shall be kept as to ensure its protection and prevents its unauthorised use, including reading, transmitting, copying or altering the information without lawful authorization, and prevents its use in violation of this Act; acts performed in the database of (communications) identification data shall be documented as to facilitate supervision and control.

(c) The database of (communications) identification data shall only be used for the purposes specified in paragraphs (1) to (4) of section 3(a)".

This reveals that the Act enables the Israel Police to require a telecommunications licensee, as defined, to transfer to it subscribers' computerised identification data and the identifying numbers of their telephone devices (or of any components thereof). The Act also facilitates requiring information about antennas the licensee uses in providing telecommunications services. In effect, the Act permits the Police to establish a database linking one's name with their telephone number and eliminates the need to telephone 144 service (which provides one's telephone number according to their name or address) or the 441 service (which provides one's name and address according to their telephone number). That said, information is kept in a confidential database and the use of that data is limited, according to section 7(c), to purposes that also warrant a judicial order, namely: saving or protecting human life, detecting, investigating and preventing offenses, detecting offenders and prosecuting

them, and seizing property under the Act. It should be noted that the database does not permit keeping any data that the Israel Police is authorized to obtain under the Act. That is, it may not keep location and traffic data.

We would say that on December 19, 2008, under his authority according to section 7(d) of the Act and with the Constitution Committee's approval, the Minister of Internal Security promulgated the Criminal Procedure (Powers of Enforcement – Communications Data) (Database of Communications Identification Data) Regulations, 5769-2008 (hereinafter: "the Regulations"). These are designed to regulate the use of the database, define those authorized to access it, guide the position of database manager, and other aspects concerning its operation and maintenance and the security of the information it stores.

35. The petitioners, and especially the Association for Civil Rights, do not object to the transmission of publically accessible telephone numbers to the Israel Police and other police entities. Their objection to the identification database is more specific and they request we restrict the ability to transmit identification data of anyone whose telephone number is unlisted to the database. They argue that the constitutional right to privacy, which includes the right to keep one's "conversation confidential", also includes the right to own a telephone number that is hidden from the public eye and the investigatory authorities. Although the petitioners do not dismiss the possibility that criminal activity will be conducted under "cover" of unlisted numbers, they maintain it is always possible to approach a court. They claim it is unnecessary to establish a database that is always open to investigatory authorities without having to obtain a court's approval for unlisted numbers. The petitioners in fact focuses on the risk of establishing a database that includes unlisted numbers accessible to any policeman or other person who works for the investigatory authority, and on the concern about information "leaking" from the database to others – inside or outside the investigatory authority – who would use the information improperly.

36. In response the State maintains first that the right to "confidential conversation" does not include the right to an unlisted telephone number, which is merely a technical possibility provided by the telephone companies as a contractual matter between them and customers. Furthermore, the state argues that even were the right to an unlisted telephone number recognized, such right does not exist vis-à-vis the investigatory and law enforcement authorities, and presumably no reasonable person really expects this to be the case. At the practical level, the State argues that even now calls made from unlisted telephone numbers to the Police call centers are not confidential to these centers. The State further warns that excluding unlisted numbers from the database that is accessible to the investigatory authorities would create a means for criminals, who wish to use unlisted numbers in criminal activity, to hide from the eyes of the Police. As to the purpose of establishing the database, the State explained that the arrangement is designed to limit the time necessary to trace a particular telephone number's owner. Without the arrangement embodied in the Act, investigatory authorities would have to reach out to the communications companies about any number in order to obtain the subscriber's identification details.

37. We do no see fit to accept the petitioners' request to restrict the use of the database. We accept the State's argument that a communication company's commitment to the customer to provide an unlisted number does not entitle the customer to confidentiality from law enforcement authorities. Moreover, it should be borne in mind that the interpretation of the database's use – like the use of the judicial arrangement – is narrow and restricts the investigatory authorities' action to specific cases only, when the information in the database is required to prevent a particular crime, trace a particular offender, save or protect human life or seize property under the Act in concrete circumstances (and see section 7(c) of the Act, which refers to sections 3(a)(1) to (4)). As analyzed above, it appears that, given the Israeli constitutional system, it is improper to interpret the Act to permit using the database for Police intelligence activity generally or for infrastructure. Given this presumption, we do not consider it justified t limit the actual transmission of particular numbers to the database to enable those who wish to conceal themselves from the eyes of law enforcement authorities to do so. Consequently, the petitioners' argument should be dismissed.

As *obiter dictum*, we briefly refer to a new argument by the Association for Civil Rights (hereinafter: "the Association") in its supplemental brief from November 16, 2008, which was not raised in the actual petition. As the argument goes, the Act's infringement is aggravated due to the Police's capability to obtain communications data automatically, without needing the communications companies' authority, by connecting online to the cellular and Internet companies' computers. According to the Association, section 13(b) of the Communications Act hints at this capability. The section enables the Prime Minister to prescribe security arrangements for transmitting data between security forces – including the Israel Police – and the communications companies. The Association relies on the fact that the General Security Service already uses such capability, and as support it presents the respondents' answer in AP 890/07, *The Movement for Freedom of Information v. The Ministry of Communications* (unpublished, November 5, 2007). The respondents there explained there are indeed secret security appendices that regulate transmission of communications data from communications companies to the General Security Service. Nevertheless, the respondents there explained that those appendices do not regulate the General Security Service's powers to obtain communications data but only the technical means to obtain them and that the powers to obtain the data are subject to the substantive law regulating them. In response, the State explained here that independently from how the data are transmitted – be it online in real time or by a specific motion – the accessible data would only be those permitted by the Act and its arrangements. It was further explained that the question about the technological way the data is transmitted is in any event of no constitutional significance. We have not found the Association's argument, which was made partially and unsatisfactorily, to constitutionally justify striking down the Act. In any event, the concern the Association raised in its argument relates to the improper use of access to the data, which is facilitated through online access to the data, rather than to actually permitting access, which is restricted, as mentioned, by the Act, with the narrow interpretation that our opinion applies to them. Clearly, should the petitioners believe that the way the data are actually transferred demonstrates the Act's

implementation beyond the proper criteria outlined or should the petitioners find evidence of improper use of the means granted to the investigatory authorities, they may take the appropriate steps.

(b) *The Proportionality of the Law As a Whole*

38. We have therefore reached the conclusion that the arrangements in the Act, including the judicial arrangement, the administrative arrangement and the keeping of unlisted numbers in the database, do meet the requirements of the Limitations Clause and do not establish cause for constitutional intervention. In addition, we would further say that an overall review of the Act and all the arrangements and balances in it also leads to the conclusion that no cause for our intervention has been established.

First, as stated in paragraph 25 of our opinion, the administrative arrangement in section 4 concerns only grave, urgent cases. Accordingly, the legislature has left the majority of the investigatory authorities' actions under the Act to address by a court through the judicial arrangement. Such a balance, insofar as actually implemented according to the obligatory criteria, ensures judicial review of the majority of cases in which investigatory authorities infringe privacy by exercising powers under the Act. As discussed, the judicial authority has a weighty responsibility to insist on limited and appropriate use of the powers granted by the Act. But as discussed, the very existence of judicial review of the main procedure for obtaining data under the Act indicates its proportionality.

It should be noted that the fact that "the usual course" is that which passes through the courts and that it is not self-evident that only in urgent, exceptional cases will the administrative course be used. Thus, for example, in the English law that deals with obtaining communications data, this distinction between emergencies and the ordinary course does not exist, and investigatory authorities can in all cases act through the administrative course without needing a judicial order (sections 25(1) and (2) of the RIPA). In particularly serious emergencies the authority may even act without written authorization at all – even administrative – and oral authorization is sufficient (as provided in the Regulations – section 3.56). On the other hand, the outlook of American law is closer to Israeli law and it lays down an administrative, alongside a judicial, course. As detailed above, the administrative course, which is regulated in §2703(c)2, Chapter 18 of the USC, enables the investigatory authority to obtain various types of communications data without judicial involvement. In this connection, by means of an administrative order, it is possible to obtain the subscriber's name, address, calls documentation, means of payment and others. Beyond the data that can be obtained under this section, a judicial order is necessary (the American law distinguishes between two types of orders). It should nevertheless be noted that insofar as our examination has revealed, it appears that American law sometimes recognizes the ability to be relieved of the primary duty to approach a court and in urgent cases permits administrative orders. When the investigatory authority seeks to use surveillance devices that enable obtaining real time data of outgoing and incoming calls from an Internet or telephone communications source (pen registers/trap and trace

devices), American law recognizes exceptional cases where a judicial order may be bypassed and an administrative order suffices: a risk to a person's life or serious injury; acts suspected as organized crime; an immediate threat to a national security interest; or an attack on a protected computer. An administrative order issued according to this arrangement is only valid for 48 hours, after which the investigatory authority must request a judge's approval again or stop using it (§3125(a) of Chapter 18 of the USC). Canadian law, too, reflects a similar approach to that of Israeli law. It provides that the usual course for obtaining communications data is by approaching a judge (sections 184 to 186 of the Canadian Criminal Code), while the administrative course is defined in Canada as an option that is available to the investigatory authorities only in rare emergencies.

Second, the Law grants different powers to different investigatory authorities and delineates their use in a way that contributes to its proportionality. Thus, while all investigatory authorities addressed by the Act – the Israel Police, the Military Police CID, the Police Internal Investigations Department of the Ministry of Justice, the Securities Authority, the Antitrust Authority and the Israel Tax Authority – are authorized to use the judicial arrangement and approach a court for an order to obtain communications data, only the Police and the Military Police CID have been empowered to follow the administrative arrangement. This distinction acknowledges that alongside the importance of enabling the other investigatory authorities to perform their duties in the best way, the most "infringing" powers are to be granted to a limited group of authorities that are used to dealing with urgent cases, whose potential need of those powers is greater. In our opinion this substantially limits the potential infringement of the right to privacy.

Again in this respect, the Act's proportionality may be inferred by reviewing similar arrangements in corresponding legal systems. Thus, English law's list of the authorities empowered to use the arrangements for access to communications data is not exhaustive. Instead, several investigatory entities are explicitly named, like the Police, the National Criminal Intelligence Service, the National Crime Unit, the Customs Authority, the Inland Revenue and also the intelligence services – and the Home Secretary is also empowered to go on to prescribe additional agencies for the purposes of the Act (see section 25 of the RIPA). It appears the powers the English law grants the various different authorities are broader than those recognized in the Communications Data Act, especially in light of the ability of the agencies mentioned to obtain communications data merely by using the administrative course, without needing a judicial order.

Third, the Act's proportionality also depends on the review to which it subjects its proper, limited implementation. This check is prescribed in section 14 regarding the Act's general use and in sections 4(d) and (e) regarding the use of an administrative order. Section 14 mandates that the Minister responsible for the relevant investigatory authority must report to the Knesset Constitution Committee as to the use the investigatory authority for which he is responsible made of the Act, including the database. Sections 4(d) and (e) respectively provide that the competent officer who has

authorized the administrative arrangement must report the order in writing; and that once every three months the head of the Israel Police Investigations and Intelligence Branch and the Commander of the Military Police CID must submit the data collected from the competent officers to the Attorney General or the Military Advocate General, as the case may be. This review is far more frequent than the review conducted by the Knesset. We would also mention that, presumably, in the course of the Attorney General's periodic review, there will be consideration for, *inter alia*, reviewing the circumstances in which communications data has been obtained under section 4 and to whether it might have been possible in those circumstances to act under section 3 and obtain an appropriate judicial order.

These mechanisms for review, coupled with the court's approval of motions pursuant to section 3, make it possible to control the Act's actual implementation and ensure the investigatory authorities limited use of the tools the Act provided them, according to the criteria detailed in our decision. Their existence makes it possible to assume that the Act's implementation would be periodically reviewed and that problems arising in such respect, as reflected from the discussion in paragraphs 31-33, will be dealt with in the best possible way. That this control is maintained and that the supervisory entities – the Attorney General and the Constitution Committee – examine in detail the reports received and the authorities' compliance with the guidelines deriving from our interpretation of the Act, as expressed by us above, must be guaranteed. It should be borne in mind that the Attorney General holds a special role in strictly ensuring that government authorities exercise their powers under the Act merely to the extent necessary in order to achieve its purposes, according to our interpretation in this decision and the criteria outlined in it.

39. We acknowledge that a statute under review is not reviewed in a vacuum. As we have shown, the existence of the Police procedure, which should be read together with the Act, affects our perception of its implementation and the view that investigatory authorities would only use it properly and intelligently. Thus, the overall arrangements contained in it display a balanced and proportional picture of the exercise of powers it grants. In addition, the other means available to the authorities – which also infringe privacy – have an effect on our perception of the Act. As said, these means now include the capability to listen to one's conversations, which are regulated and limited under the Secret Monitoring Law, and the ability to obtain information by implementing section 43 of the Criminal Procedure Ordinance. This means the Police, in fighting crime, has various resources that, to some extent, infringe privacy. The relevant Act joins those resources and apparently specifically within its scope the State has come a long way towards safeguarding the constitutional right to privacy. Given the restrictions detailed above we can see it as a means that does not infringe the systemic balance between the need to fight crime effectively and maintain public order, on the one hand, and the right to privacy and dignity to which everyone is entitled, on the other hand. It is to be expected that by adding more tools in the future to be available to investigatory authorities, the legislature will maintain the internal balance of each tool as well as the systemic balance, considering all the existing resources recognized by law.

In this context we would also mention that the comparison with various arrangements the world's countries have adopted must not be made in a vacuum either; rather, how the means for obtaining communications data are integrated into the general legal system should be analyzed. Thus, for example, countries where the ability to collect communications data in particular crimes is limited – like Canada and England (partially), which limit the list of offenses in different ways – at the same time make extensive access to communications data available. Thus, English law does not require authorization by a judge in order to collect communications data, and Canadian law makes obtaining communications data possible when demonstrating a vague, general cause. The comparison with different systems and their approach to the means for collecting communications data, as adduced above in the relevant contexts, leads to conclude that even were different countries to choose different balances, the balance in the Act under review is not unreasonable compared to the balances adopted in countries with similar legal systems to Israel's, and which contend with similar challenges regarding technology, their battle against crime and in protecting privacy.

In view of all the above, we have reached the overall conclusion that the Act – together with its arrangements and their interpretation in our decision – does not infringe the constitutional right to privacy to beyond necessary.

Inadmissibility of Evidence

40. Before concluding, we believe it is appropriate to consider another issue the petitioners raised, namely the admissibility of evidence collected according to the Act in legal proceedings. The Israel Bar, which is the petitioner in HCJ 9995/08, asks that the Act stipulate that obtaining communications data in violation of the Act could not produce evidence that would be admissible in legal proceedings. Furthermore, it requests we add a requirement for the use of evidence procured through the administrative proceedings in section 4 of the Act, whereby a court would retroactively approve the competent officer's permit before the communications data obtained through the administrative order may be used as evidence in court.

41. Let it immediately be said that we do not find the petitioners' arguments in this respect substantial and do not see fit to grant the relief sought here, for several reasons. First, we would mention as our premise that the majority of statutory arrangements in our legal system do not include specific rules for inadmissibility (see CrimA 5121/98, *Private Refael Isascharov v. The Military Prosecutor*, IsrSC 61(1) 461, 524-525 (2006) (hereinafter: "Isascharov") and also compare CrimA 115/82, *Heil Muadi v. State of Israel*, IsrSC 38(1) 197, 262 (1984)). Consequently, the absence of an inadmissibility rule in the Communications Data Act does not *per se* indicate that the Act is constitutionally flawed. Moreover, we would note there are exceptions to the general rule about the lack of inadmissibility provisions in most statues in Israeli law as a limited number of statutes do include such provisions: section 32 of the Protection of Privacy Act, section 13 of the Secret Monitoring Act and sections 10A and 12 of the Evidence Ordinance [New Version], 5731-1971.

As to the Protection of Privacy Act, section 32 of that law already prescribes that material unlawfully obtained while infringing privacy is inadmissible as evidence. As the section states:

> *"Material Inadmissible As Evidence*
>
> 32. Material obtained while committing an infringement of privacy shall not be used as evidence in court without the consent of the injured party, unless the court, for reasons which shall be recorded, permits such use or if the infringer, as a party to the proceeding, presents a defense or enjoys exemption under this Act."

Consequently, without ruling on the relationship between the inadmissibility section of the Protection of Privacy Act and conduct under the Communications Data Act, material obtained in violation of the criteria concerning the Communications Data Act might be subject to the inadmissibility provision of the Protection of Privacy Act. Insofar as the Secret Monitoring Act's inadmissibility rule, as we have already held above, we do not find it possible to analogize between the two statutes and the fact that the Secret Monitoring Act includes a specific inadmissibility rule does not make it necessary to adopt a specific inadmissibility rule in the Communications Data Act too.

Moreover, as we have already held many times in the past, since the 1980s our legal system has been marked by moving from rigid rules of admissibility towards a substantive examination of evidence. We acknowledge this approach prioritizes the court's substantive review of evidence over disqualification. Nevertheless, this move has been tempered in recent years and because defendants' basic rights in criminal law were increasingly recognized, a doctrine of relative inadmissibility was adopted in Isascharov. Under this doctrine a court has discretion to rule on the admissibility of evidence that has been unlawfully obtained, depending on the specific circumstances of the case. The rule in Isascharov was summed up as follows:

> "Where in the past the case law in our legal system held that evidence admissibility is not examined by how it was obtained because the interpretive weight in such context was placed on the purpose of uncovering the truth and fighting crime, a more flexible balance is now sought. It takes into account the duty to protect the defendant's rights and the fairness and integrity of the criminal procedure. The proper balance between all the competing values and interests in this particular respect leads to the adoption of a doctrine of relative inadmissibility, whereby a court would have discretion to rule on the admissibility of evidence that has been unlawfully obtained on the merits of the actual circumstances of every case and according to the criteria below" (Id, at 546).

Given this legal framework, we have, as mentioned, not considered it proper to grant the petitioners' motions and we have certainly not found that the absence of a

specific inadmissibility rule in the Act justifies constitutional intervention. Clearly, insofar as a defendant seeks to assert that material that was obtained under the Act is inadmissible evidence, he may so argue during the judicial proceedings and the court adjudicating the case would review these claims. We do not find this arrangement should be augmented by a specific provision as to evidence obtained under the Act, as opposed to any other evidence allegedly unlawfully obtained. In terms of a requirement to obtain retroactive approval of administrative orders that were duly issued under the Act, to the extent we held the Act and the procedures under it are constitutional, it is inappropriate to hold that they should be bolstered by requirements as to how investigatory authorities may use them in legal proceedings.

Conclusion

42. The modern reality in which we live and the technological innovations that accompany it give the citizens of the world – who can afford it – means of communication that are constantly refined and that facilitate easy, quick transmission of information over great distances. On the one hand, this reality has made our world a place where a great deal of private information about the individual moves freely – frequently with the consent of that individual – in the public sphere. On the other hand, this reality has become a convenient platform for negative elements and criminals who wish to use such technology for their own purposes. Countries around the world, including Israel, have realized that these changes can be harnessed to improve their enforcement capabilities and the quality of life for their residents. The Act challenged by these petitions is Israeli law's regulation of how law enforcement may use sophisticated technology. As discussed at length above, enforcement authorities should have appropriate tools to facilitate law enforcement in the changing reality. Additionally, undoubtedly these moves may potentially infringe greatly on residents' privacy. This reality requires developing complex arrangements that properly weigh the overall interests at stake. Having carefully reviewed the overall arrangements of the Communications Data Act and its procedures, we have reached the overall conclusion that, considering the proper interpretation regarding the exercise of the powers the Act prescribes – an interpretation which essentially calls for limited implementation strictly when necessary – we see no cause for constitutional intervention. Nonetheless, as we have emphasized time and again, enforcement authorities are under a substantial duty to exercise their powers with prudent discretion and closest attention to the fact that the infringements caused by the Act should be executed only to the necessary extent and degree. Moreover, the Knesset and the Attorney General, who are legally charged with maintaining regular review over how much the Act is used, hold great responsibility in this respect. The same applies to courts reviewing motions for obtaining communications data under the Act. We assume, and trust, that all the authorities involved in implementing the Act will take the strictest care to ensure the powers the legislature granted them are not exercised unnecessarily and that they are used following the limiting criteria delineated in our decision.

For the sake of clarity, we would therefore sum up our interpretive findings regarding the Communications Data Act: first, as to the exercise of the powers in both

section 3 and section 4, we held that they should be interpreted so that obtaining data under the Act is only permissible where it is necessary for a specific, concrete purpose, like an investigation of a particular occurrence regarding a specific suspect or victim, as opposed to executing the Act for general purposes of detecting offenders and preventing crime. Second, regarding exercising the power in section 4 of the Act, we held this should be interpreted so that a permit obtaining communications data is only sparingly permissible, in extreme cases, in order to deal with offenses that require it and only where because of the urgency it has become clear that it impossible to obtain a court order under section 3. This is when the reason for not approaching a court is because of circumstances involving saving life or other serious factors, always considering a range of factors, including that the subscriber is a professional, the extent of his involvement in the offense, the type of data sought, the degree of urgency, the gravity of the offense and other similar considerations. To the extent journalists are concerned, we have found that the restrictions on the use of orders, as reflected in the procedure concerning section 4, are mandated by the Act's purpose and the balances the procedures reaches in implementation. Accordingly, when the subscriber is a journalist, who is not the victim or is not suspected of the offense, a motion under section 4 to obtain his communications data of the traffic data will not be approved.

43. Given the above and subject to the restrictions and limitations outlined in this decision as to the proper exercise of powers under the Act, we found no constitutional cause for our intervention. The petitions are dismissed. In the circumstances, there will be no order for costs.

Justice E. Arbel

1. The petition centers around the boundaries of the right to privacy as a constitutional right. Technological innovations raise concern that the State will gather and use extensive information of nationals and residents, and this requires adapting the law to this possible harm. In her opinion, the President reviews extensively and in great detail whether the balance the legislature strikes in the Criminal Procedure (Powers of Enforcement – Communications Data) Act, 5768-2007 (hereinafter: "the Act") meet the criteria of constitutionality according to our legal system. I agree with her unequivocal conclusion that the Act does infringe the right to privacy. Nevertheless, as stated, the Act neither permits actual listening to conversations or reading messages nor does it permit disclosure of the contents of a person's conversations. I also agree that the Act meets the criteria of proportionality accepted in our jurisprudence and does not infringe the constitutional right to privacy to an extent beyond necessary. Constitutional cause therefore for this Court's intervention does not arise. I believe that the inability to obtain communications data would place enforcement authorities at a disadvantage compared to offenders. I agree with my colleague the President's interpretive findings and reasoning as to the execution of the powers under sections 3 and 4 of the Act. Nevertheless, I find it proper to add one point of reference.

2. I would add what is seemingly self-evident about section 4 of the Act, which permits a competent officer to grant a permit to obtain communications data without a

court order in urgent cases in order to prevent a felony, to detect its commission or to save human life, when a court order under section 3 cannot be obtained in time under the circumstances. Section 4(b) of the Act limits such permit to a period of no more than 24 hours. Nevertheless, the Act's language does not expressly preclude the permit's renewal by a competent officer at the end of such period or some time thereafter. In my opinion, section 4(b) should be construed as precluding that possibility and as requiring the competent authority to approach a court for an order under section 3 of the Act to the extent it is necessary after the initial period has expired – namely after 24 hours. This interpretation is warranted so that the infringement of the right to privacy does not to exceed the necessary. I would also note that it would be proper, in my opinion, to consider inferring from section 5(d) of the Secret Monitoring Law, 5739-1979 about the court's retroactive approval of permits issued in urgent cases without a court's approval. Although section 4 of the Act prescribes arrangements that would permit the Attorney General and the Military Advocate General's review of that section's application, in my opinion that is inadequate and the court's review of the section's implementation should also be required through retroactive approval of the permit awarded.

As said, I concur with the President's comprehensive opinion and reasoning.

President U. Grunis

I agree that the petitions should be dismissed as proposed by my colleague, President (Ret.) D. Beinisch.

Justice M. Naor

I join the comprehensive opinion of my colleague, President (Ret.) D. Beinisch.

Justice E. Hayut

I join the opinion of my colleague the President and her conclusion that subject to the reservations detailed in her opinion as to the proper exercise of the powers granted by the Criminal Procedure (Powers of Enforcement – Communications Data) Act, 5768-2007, the Act meets the criteria of proportionality under the case law and does not infringe the right to privacy unconstitutionally.

Justice H. Melcer

1. I join the comprehensive opinion of President (Ret.) D. Beinisch (hereinafter: "the President") in respect to the proper constitutional interpretation of sections 3, 6 and 7 of the Criminal Procedure (Powers of Enforcement – Communications Data) Law, 5768-2007 (hereinafter: "the Communications Data Collection Act" or "the Act"). Nevertheless, I find myself at issue with the President on two matters:

(a) The protection that should be given in the context of the Law to someone in respect of whom professional privilege applies by law, including case law (hereinafter: "professional privilege"); and

(b) The proper constitutional interpretation of section 4 of the Act and the limitations of its deployment.

My opinion on both these issues is expressed below. I would immediately say that my view leads to a constitutional-interpretative conclusion that a competent officer, as defined by section 1 of the Act, cannot act under section 4 of the Act where professional privilege *prima facie* applies. The only way to try to obtain communications data in such situations is approaching a court and securing its authorization according to section 3 of the Act (especially section 3(b)), subject always to the provisions of law (including case law).

I shall now present the reasoning of my said approach and give details in order.

The Scope of Professional Privilege in the Context of the Communications Data Collection Act and the Constitutional Rights Involved, upon which the Privilege is Based

2. The President states (at the beginning of para. 10 of her opinion) that it was held in the past that professional privileges "essentially extend to the content of the conversations between the professional and the privileged person but not to the very existence of a relationship with the professional person, and the purpose of the privilege is to allow the privileged person a realm of free communication between him and the professional." Therefore, the President believes that the Communications Data Collection Act does not in fact infringe privilege, apart from journalistic privilege because, as she sees it, the Act in any event does not permit the obtaining of substantive data, to which the privilege applies.

3. We can see that this method – which distinguishes between the conversation's substance (which is privileged) and the information around the conversation's existence and the identity of the parties to it, which is not privileged (according to the argument) – has a significant effect on the consequences of reviewing the whole Act because it impacts the precursory determination of the scope of the constitutional rights that are infringed by the Communications Data Collection Act. Indeed, the conclusion that the first stage of the constitutional analysis, which concerns identifying the scope and force of the constitutional right and its limits, naturally has a significant effect on the second stage of that analysis, which deals with reviewing the constitutionality of the infringement on the constitutional right or of the limitations imposed upon it (see: Aharon Barak, *Proportionality in Law* 43-48 (2010)).

I shall therefore start my enquiry into the key preliminary question as to the relevant privileges and the constitutional rights involved in the whole, an issue where my opinion differs from the position presented by the President.

4. I agree that as a point of departure the distinction between "form" and "substance" should be respected so that the core of the privilege should first apply to the information concerning the contents of conversations between the privileged party and the professional. However, there are cases – and current technological development demonstrates that the same is becoming more and more prevalent – where the core of the privilege, as defined above, radiates outwards and should also protect information, which although *per se* constitutes only the "form" of the communication, does in the relevant context provide tools for the prohibited disclosure of privileged information. In such cases, that "technical" data, which is not apparently originally privileged, falls within the privilege because its disclosure provides access to protected information. What is important here is that in such cases (which, as noted, are recently not so few) obtaining communications data might infringe professional privilege.

Hence, the constitutionality of the Data Communications Collection Act's provisions, for a provisional order was issued, not only regarding journalistic privilege but also regarding the privilege of other professionals, within the meaning of section 3(d)(7) of the Act. I shall now express my position as to two privileges: attorney-client privilege and doctor-patient privilege. I shall then explain what sets journalistic privilege apart and refer to the constitutional rights in all these contexts and their implications to the Act's interpretation.

Attorney-Client Privilege and the Constitutional Rights upon Which It Rests

5. It is common to believe that a particular method of payment by a client to an attorney – in cash or by check etc. – ordinarily falls into the category of information that is not privileged. In the United States, this distinction gives rise to certain difficulty that impacts the instant case. The enforcement authorities there have discovered that offenders who deal in smuggling dangerous drugs habitually pay for the services they use (that is to say lawful services, including legal services) in cash. Enforcement authorities therefore tried to use this and have attempted to inspect lawyers' tax returns in order to find large payments of professional fees in cash and the identity of the payers. The lawyers have argued that privileged information, which should not be disclosed, is involved. The conclusion reached in the United States is that, generally, information concerning the method of a particular client's payment and his identity are not privileged but such information can enjoy privilege where the information:

> "reveals the motive of the client in seeking representation, litigation strategy, or the specific nature of the service provided" (Chaudhry v. Gallerizzo, 174 F. 3d 394, 402 (4th Cir. 1999); Diversified Group, Inc. v. Daugerdas, 304 F. Supp. 2d 507, 514 (S.D.N.Y. 2003)).

That is then one typical way in which the privilege can radiate outwards from its core to information that is not *prima facie* privileged and that is indeed the way in which matters have also been interpreted in the legal literature there:

> "The privilege protects an unknown client's identity where its disclosure would reveal a client's motive for seeking legal advice. Here extending the privilege to the client's statement of identity is a means to the end of protecting the confidentiality of the client's more substantive communications with the attorney" (Edward J. Imwinkelried, *The New Wigmore: Evidentiary Privileges* 746 (2nd Ed., 2009) emphasis added – H.M.; see also Thomas E. Spahn, *The Attorney-Client Privilege and the Work Product Doctrine* vol. 1 93 (2007)).

In Israel, although it is usual to think that the privilege does not apply to the client's name, it has been maintained that this position is not free of difficulties similar to those described above (see, Dr Gabriel Kling, *Ethics in Advocacy* 418-419 (2001)). It should also be noted that it was recently held in this context that the obligation imposed on certain attorneys in Israel to include clients' names in their periodic VAT returns "is not a disproportionate infringement of the client's privilege vis-à-vis his relationship with the attorney." Nevertheless, that finding was qualified: "if a concrete problem arises regarding the privilege, the client's right to argue for privilege is reserved." (HCJ 115/11, *Adv. Cassouto v. The Tax Authority* (unpublished, April 30, 2012)).

6. It should be noted here that attorney-client privilege, which is regulated in Israel by section 90 of the Israel Bar Act, 5721-1961 and section 48 of the Evidence Ordinance [New Version], 5731-1971 (hereinafter: "the Evidence Ordinance"), preceded the Basic Law: Human Dignity and Liberty, but since its legislation this privilege apparently also has constitutional element. Attorney-client privilege now derives, at the constitutional level, from the constitutional right to dignity (sections 2, 4 and 11 of the above Basic Law), the constitutional right to liberty (sections 5 and 11 of the above Basic Law) and the right to due process, which was recognized in the case law as a (derivative) constitutional right. See and compare the statement by then Justice D. Beinisch in CrimA 5121/98, *Isascharov v. The Chief Military Prosecutor*, IsrSC 61(1) 461, 560-561 (2006); Mot.Crim 8823/07, *John Doe v. State of Israel*, para. 16 of Deputy President E. Rivlin's opinion (unpublished, February 11, 2010).

7. It should also be mentioned here that the Constitutional Court of Germany recently heard a petition similar to those before us here (which was brought by the German Bar and German Press Association against a corresponding statute that had been enacted there, regulating the collection of communications data). The German Constitutional Court held – in a judgement that was handed down on October 12, 2011 – that absolute privilege should be granted in respect of the gathering of communications data from a practising lawyer, on the basis of attorney-client privilege (which there is based on the constitutional right to dignity) and it also recognized partial privilege (which can be lifted by judicial order) over collecting communications data from journalists. (See BVerfG, 2. Senat, Az: 2 BvR 236/08, 2 BvR 422/08).

A similar constitutional approach was adopted in Britain in *R. (On the Application of Morgan Grenfell & Co. Ltd) v. Special Commissioner of Income Tax*

[2003] 1 AC 563 (hereinafter: "MG"). See also Phipson, *On Evidence* 658 (17th ed, 2010). Compare the judgment of the European Court of Human Rights, *Kopp v. Switzerland* [1998] 27 EHRR 91. See on the other hand *In Re McE* [2009] UKHL 15 and criticism of that judgment by Simon McKay, *Covert Policing – Law and Practice*, pp 277-279 (2011).

Doctor-Patient Privilege

8. When a doctor practices exclusively in a particular medical field a situation might arise where the very contact with that doctor – even though the substance of the contact or treatment is not disclosed – will enable a third party to deduce information concerning the purpose underlying the contact and infringe the privilege that governs the relationship between doctor and patient. Thus, for example, it was held in this context in HCJ 447/72, *Ismachovitz v. The Investigatory Assessing Officer*, IsrSC 27(2) 253 260 (1973) (hereinafter: "Ismachovitz"), as also mentioned in the President's opinion:

> "… Here the petitioner states that because of his specific practice in the sphere of sterility and impotence, the disclosure of patients' names and others who have visited him, such as sperm donors for artificial insemination, merits privilege because those involved would not go to a doctor if they perceived the risk that it would become known. […] I am willing to assume that there may be special cases, where even the identity of the patient will fall within the scope of a privileged confidence under section 49 of the Ordinance, although I dare to doubt whether the petitioner's practice does indeed require such extension of the protection of privilege".

As mentioned, in the circumstances of Ismachovitz it was held that the identity of the person going to the doctor was not protected, *inter alia* because the petitioner there practiced in several spheres (and for other legal reasons). However, this conclusion does not derogate from the more general perception that the rigid distinction between the very contact and its substance is problematic in many cases, especially in areas concerning telecommunication. See *Constitutional Rights and New Technologies – a Comparative Study*, 277-278 (Ronald Leenes, Bert-Jaap Koops, Paul De Hert, Ed., 2008).

Furthermore, once the Patient Rights Act, 5756-1996 was legislated (especially if we interpret it in light of Basic Law: Human Dignity and Liberty, which preceded it), the patient's right to privacy gained paramount status and was raised to constitutional level. Section 19(a) of this Act provides in our context as follows: "a clinician or medical institution worker shall keep secret <u>all information relating to the patient</u> that comes to his knowledge in the course of his duty or in the course of his work" (emphasis added – H.M.).

Nevertheless, there is still a certain difference so far as we are concerned between the professional privileges that are regulated, for example in the Evidence

Ordinance (all of which can be constitutionally justified one way or another) and journalistic privilege (which is considered to be a creature of case law, with specific characteristics). This difference was also highlighted in these petitions and the President also acknowledged it. We shall immediately deal with this at greater length.

The Journalistic Privilege and the Constitutional Rights upon Which It Rests

9. In paragraph 10 of her opinion, the President writes as follows:

> "As the State also agreed, with regard to journalists, the very identity of the person who contacts a journalist can constitute part of journalistic privilege because it may expose the journalist's source despite the protection given to such source."

This Court has considered the protection granted to a journalist's source. In the case of Tzitrin (MA 298/86, *Ben Zion Tzitrin v. The Disciplinary Tribunal of the Israel Bar, Tel Aviv District*, IsrSC 41(2) 337 (1987) (hereinafter: "Tzitrin")), President M. Shamgar stated:

> "The protection of the sources of information necessary for the performance of the journalist's function, including protecting the relationship of trust on the basis of which information is given in return for an assurance that the source not be disclosed, is therefore a public interest and not the particular interest of the relevant newspaper or journalist" (ibid, p 358).

Since Tzitrin, this view has been an axiom of Israeli constitutional law. Nevertheless, the journalist's privilege has several unique elements compared to other professional privileges and they are set out below –

(a) As already mentioned, it is the result of case law, while the others are statutory.

(b) It is relative (like some of the statutory privileges), unlike, for example, the privilege covering evidence concerning the attorney-client relationship (section 48 of the Evidence Ordinance) or evidence presented by clergymen (section 51 of the Evidence Ordinance), which are absolute. For these, the Evidence Ordinance does not prescribe a balancing formula and courts have not been granted power to order revoking the privilege. See: LCA 5806/06 *The Estate of Michael Namirovski, Deceased v. Shimko*, paras. 6-7 of Deputy President E. Rivlin's opinion (unpublished, June 13, 2007); HCJ 844/06 *Haifa University v. Prof. Avraham Oz*, para. 11 of Justice E. Hayut's opinion (unpublished, May 14, 2008) (hereinafter: "Haifa University").

(c) It blocks evidential expression in judicial or investigative proceedings – with the intent of making journalistic information public. The other privileges that apply, for example, in respect of treatment-oriented professions, like

lawyers, doctors, psychologists or social workers, preclude the flow of information (to the court) in order to enable the individual privately to put to the professional all the information necessary for his treatment. On the other hand, journalistic privilege blocks evidential expression in judicial or investigatory proceedings specifically with the intention of making matters public and ensuring the public's right to know. See: pp viii and ix of the work by Yisgav Nakdimon, *Precluding Expression in Order to Permit Expression – Suggested Thought Process for Fashioning the Scope and Protection of Journalistic Privilege in the Constitutional Era* (Ph.D. thesis, under the supervision of Prof. Ariel Bendor, The Faculty of Law, Haifa University, 2012 (hereinafter: "Nakdimon").

(d) Unlike the other privileges, it is likely to be infringed *per se* on disclosure of the journalist's communications data, which is likely to expose the identity of his sources of information, which is at the very heart of the privilege and not the mere periphery of the right. Hence, it should be acknowledged that not only the name of the source, but any detail or information that might lead to his identification should fall within the scope of journalistic privilege. See: Nakdimon, id, at 153-154, 276-277.

10. The journalist's privilege is therefore one of the means that guarantee freedom of the press, and constitutionally it is as though it were drawn from the freedom of expression, which is an independent constitutional right that is "at the very heart of democracy" (CrimA 255/68, *State of Israel v. Ben Moshe*, IsrSC 22(2) 427, 435 (1968)). Other approaches maintain that the freedom of expression itself depends upon a certain degree of privacy, which permits one's autonomous and original development. See: Stephen Breyer, *Active Liberty* 62-63 (2008); Ruth Gavison, *Privacy and the Limits of the Law* (Yale L. J. 475 (1980). For a summary of the different perspectives on this, see also: CA 751/10, *John Doe v. Dr Ilana Dayan-Orbach*, paras. 61-66 of Deputy President E. Rivlin's opinion (unpublished, February 8, 2012) (hereinafter: "Dayan").

11. The other view does not see journalistic privilege as rooted in the doctrine of free expression but bases it directly on the rationale of individual privacy and confidentiality of conversations, that are now constitutional values protected under section 7 of Basic Law: Human Dignity and Liberty (to be precise, the confidentiality of conversation would also appear to include the confidentiality of the parties to the conversation, rather than just its content). Hence, according to this view, journalistic privilege enables the reporter's source to maintain his anonymity in the world outside the "confidential domain" between the two (see: Michael Birnhack, *Control and Consent: the Notional Basis of the Right to privacy*, MISHPAT U'MIMSHAL II, 63-64 (2007) (hereinafter: Birnhack, Control and Consent); Michael Birnhack, *The Private Domain: the Right to Privacy between Law and Technology*, 121-122 (2011) (hereinafter: Birnhack, Private Domain); Nakdimon, at 141-143). In this context anonymity is perceived as part of the right to privacy since "it enables a person 'to act in peace' and avoid personal exposure and the giving of information about himself that

he does not wish to give… Anonymity gives a person control over information about himself… and prevents 'gazing' into his privacy". (See LCA 4447/07, *Mor v. Barak ETC (1995) International Telecommunication Services Ltd*, para. 13 of Deputy President E. Rivlin's opinion (unpublished, March 25, 2010); see also Nakdimon, p 141).

12. All the above indicates that the journalist's original privilege can also be based on the value of human dignity, enshrined in sections 2, 4 and 11 of Basic Law: Human Dignity and Liberty, because such privilege contributes to safeguarding the freedom of expression, which in turn is embodied in the doctrine of human dignity (see: CA 105/92, *Reem Contracting Engineers Ltd v. Nazareth Elite Municipality*, IsrSC 47(5) 189 (1993); HCJ 2481/93, *Dayan v. The Commander of the Jerusalem District*, IsrSC 48(2) 456 (1994); PPA 4463/94, *Golan v. The Prison Service*, IsrSC 50(4) 136, 152-153 (1996)).

To be exact, another constitutional track, which also has certain support, in fact finds the constitutional embodiment of the freedom of expression in the right to liberty, as protected under sections 5 and 11 of Basic Law: Human Dignity and Liberty (see, for example, the paper by Dr Guy E. Carmi *Dignity – the Enemy from Within: a Theoretical and Comparative Analysis of Human Dignity As a Free Speech Justification*, 9 U. PENN. J. CON. L. 957 (2007) (hereinafter: "Carmi I"); Guy E. Carmi *"Dignitizing" Free Speech in Israel: the Impact of the Constitutional Revolution on Free Speech Protection* 57 MCGILL L. J. (forthcoming 2012) (hereinafter: "Carmi II"). However, this possibility – which has not yet become entrenched in the Israeli legal system – does not directly impact the analysis here and there is therefore no need to consider it at length. Furthermore, as mentioned in LCA 10520/03, *Ben Gabir v. Dankner* (unpublished, November 12, 2006), there is in any event a certain natural proximity between the separate doctrines of liberty and dignity, which *inter alia* also finds expression in protections of free expression: "the freedom of expression is the mother of freedoms. It is also the most fragile of them. It is the first to be infringed but the infringement never stops there. All the freedoms fall together with it. Its fall marks the end of human dignity. Human liberty – man's dignity. Human dignity – man's liberty" (emphasis added – H.M.; see also in this respect Carmi I, pp 966-967; Dayan para 66).

Interim Summary

13. The analysis so far demonstrates that the possible infringement by the Communications Data Collection Law of the protected privileges is not limited merely to journalistic privilege and it might also extend to other privileges that are embodied in the Evidence Ordinance and other provisions of law, or those the case law has or will recognize in the future (see: section 3(d)(7) of the Act. See also Haifa University, bottom of para. 19 of Justice E. Hayut's opinion (unpublished, May 14, 2008); HCJ 793/05, *Bar Ilan University v. The Jerusalem National Labor Court,* paras. 11-14 of President D. Beinisch's opinion (unpublished, January 31, 2011)).

Professional privilege therefore promotes the interests of a person involved in a variety of relevant spheres (religion, medicine, law and the like), without concern that his sensitive, personal information will be disclosed (see: Birnhack, Control and Consent, p 34; Isaac Amit, *Admissibility, Confidentiality, Privilege and Protected Interests in Civil Law Discovery Proceedings – An Attempt to Impart Order* in URI KITAI BOOK 247 (Ed. Boaz Sangero, 2007)).

As aforesaid, this concept affects constitutional review because in my opinion infringing the privileges constitutes at least an indirect infringement of the constitutional rights to dignity, liberty and privacy.

14. In view of all this and considering the compound infringement of the constitutional rights of privileged persons, which is at stake here, it seems appropriate to ease the sharp distinction between "substance" and "form" in the context of privileges and the communications that include or encompass them. Indeed, "cohesion between the media and the collapse of the distinction between content and communications data requires a new legal framework for protecting privacy, which is not based on a dichotomy like its predecessor but on a continuum of situations classified according to the degree of risk they pose to privacy" (see: Omer Tene, *Look at the Pot and See What Is inside: Communications Data and Personal Information in the 21st Century"* in LEGAL NETWORK: LAW AND INFORMATION TECHNOLOGY 287, 313 (Ed. Niva Elkin-Koren & Michael Birnhack, 2011)).

I shall now then move on to analyze the constitutional validity of the provisions of the Communications Data Collection Act under review here, in light of my conclusions above. Since I do agree, as noted, with the President's approach as to the constitutionality of sections 3, 6 and 7 of the Communications Data Collection Act, my review below will center on the constitutionality of the "administrative course" prescribed in the Act, and the boundaries that should, in my opinion, be set for it.

Summary Review of the Constitutionality of Section 4 of the Communications Data Collection Act

15. Section 4 of the Communications Data Collection Act establishes a "course" for obtaining permits under the Act, which is reserved for "urgent cases." The main characteristic of this "course" is that the entity authorizing the permit is not a court but a "competent officer," as defined in section 1 of the Communications Data Collection Act. It stands to reason – and the President also agrees – that such "administrative course" involves greater infringement of constitutional rights than the "legal course" since a permit to obtain communications data is granted here by an administrative entity – the competent officer – who is asked to do so by another administrative entity (sometimes within the same organization as the competent officer), without having to justify to the judicial authority the reasons for awarding the permit.

Indeed, there is a presumption that the administrative authority acts properly and presumably section 4 of the Communications Data Collection Act will only be used

where the competent authority believes – in good faith – that this is essential. However, even given this, it does appear to me that, as a society, it is our duty to limit such situations as far as possible since "without judicial review of the executive authority, the separation of powers is undermined and with it man's liberty is impaired and the fundamentals of the free regime are harmed" (see: HCJ 294/89, *The National Insurance Institute v. The Appeals Committee under Section 11 of the Victims of Hostile Action (Pensions) Law, 5730-1970*, IsrSC 45(5) 445, 450 (1991); see: Amnion Rubinstein, Barak Medina, THE CONSTITUTIONAL LAW OF THE STATE OF ISRAEL vol. I 174 (2005)). Compare with the decision of the Constitutional Council in France, No. DC 2005-532 of January 19, 2006.

16. This inherent problem of section 4 is resolved to some extent by the fact that some of the elements of the "the administrative course" detailed in it are narrower than "the judicial course" regulated in section 3 of the Act and also because it is motivated by the situation's urgency.

Nevertheless, as I see it, "the administrative course" is not appropriate for contending with professional privilege. I shall below explain the reasons for this approach, which differs from my colleague's opinion.

17. In paragraph 25 of her opinion, the President states that "in the absence of such infringement [in the proportionality of the Communications Data Collection Law – of the privileges, apart from journalistic privilege; the additions in square brackets are mine – HM], prima facie it cannot be said section 4 does not refer to professionals *per se* it must be struck down for unconstitutionality." The President also believes the difference between the purposes of the separate "courses" established in the Communications Data Collection Act and the fact that section 4 of the Act is reserved merely for urgent cases can all justify infringing the constitutional rights (to privacy) of professionals, including journalists (albeit with more extensive reservations regarding the latter).

In this respect I would adopt a different line and, in my opinion, even in urgent cases, greater (albeit not absolute) weight should be attributed to the constitutional rights of the beneficiaries of professional privilege that may only be infringed, if at all, through a judicial order under section 3 of the Act, which *inter alia* meets the conditions of the Limitations Clause (my opinion in CA 9183/09, *The Football Association Premier League Ltd v. John Doe* (unpublished, May 13, 2012). I reach this conclusion by giving a restrictive constitutional interpretation to the provisions of section 4 of the Communications Data Collection Act and the structure of the Act generally but not by invalidating the section, as the petitioners seek. The main reason I am adopting this method of interpretation is twofold –

(a) Invalidating a provision of statute is indeed a last resort and before doing so it should be attempted to resolve the difficulties, if at all possible, by interpretation.

(b) Invalidating a section of the Act opens up the possibility for another inadequate normative arrangement to be enacted in the future, while interpreting the section now resolves the constitutional difficulty once and for all.

See: HCJ 9098/01, *Genis v. The Ministry of Construction and Housing*, IsrSC 59(4) 241 (2004) – in the opinions of President A. Barak and then Justices M. Cheshin and D. Beinisch there.

My willingness to interpret, rather than strike down, is thus my joining the President's. Nevertheless, as for the proper interpretation, I take issue with my colleague's opinion as I shall immediately explain.

18. The President believes that the narrow arrangements in section 3 of the Communications Data Collection Act can also be reflected in implementing section 4 of the Act as relevant factors that must be considered when exercising the discretion (see para. 26 of her opinion). She also states (in paras. 27-28 of her opinion) as a factor in support of her opinion that the State in fact accepts that position and it is reflected in the Police procedure that regulates the Act's use (hereinafter: "the procedure").

I myself believe that neither the State's concession nor the procedure should carry determinative weight in this context. Although the State now agrees that the section 4 of the Act should be implemented somewhat narrowly, nothing lasts forever and in any event this concession (and the procedure based on it) does not constitute a meaningful constitutional factor, but at most alters the administrative framework. It is also deficient in that it involves something of a prohibited secret enactment. Compare: CA 421/61, *State of Israel v. Haaz*, IsrSC 15 2193, 2204-2205 (1961); LPrisA1127/03, *State of Israel v. Klein*, IsrSC 48(3) 485, 515 (2005).

Hence, I cannot accept the President's position that "naturally, a change in the authority's conduct could also lead to a material change in the balance embodied in the Act. Such a change would give rise to new cause to challenge the Act, certainly at the administrative level and perhaps even the constitutional level" (see para. 30 of her opinion). As I see it, the infringement of privilege is currently happening and there is therefore no reason to postpone constitutional review until such time as the administrative authority departs from its narrow approach, *a fortiori* since in my opinion that approach is inadequate. Hence, as I see it, considering the great role of privileges in safeguarding the constitutional rights detailed above, it is appropriate to hold that interpretatively the "course" for dealing with requests concerning professionals is only in section 3 of the Communications Data Collection Act and constitutes specific law in such respect. Section 4 of the Communications Data Collection Act cannot therefore be used in order to request an "administrative permit" concerning professional privilege.

I shall clarify this conclusion below and commence by detailing the relevant constitutional context.

19. In CA 6821/93, *United Mizrahi Bank Ltd v. Migdal Cooperative Village*, IsrSC 49(4) 221, 265 (1995), President (Ret.) M. Shamgar held as follows (emphasis added – H.M.):

> "The theoretical point of departure is that the legislature, wishing to alter or infringe a protected right, does so by express provision or clear contradictory determination in the language of the new provisions that conflicts with what preceded it. In any event there should be an attempt to implement statutes that cause this issue by trying to reconcile them. Consequently, the interpretive presumption is that a right protected by an ordinary statute cannot be changed or infringed by subsequent ordinary legislation unless otherwise stated or implied."

In the instant case I believe the argument was established that section 4 of the Communications Data Collection Act – if implemented against professional's privilege – would infringe their constitutional rights. Such infringement is not done by express language but impliedly and it does not constitute a "clear contradictory determination" in the words of President (Ret.) M. Shamgar. President D. Beinisch and Justice. E. Hayut adopted a similar approach in HCJ 10203/03, *National Commander Ltd. v. The Attorney General* (unpublished, August 20, 2008). It should also be noted that based on a similar perception it was held in Britain, in MG, that:

> "Legal professional privilege is a fundamental human right long established in the common law… The courts would ordinarily construe general words in a statute, although literally capable of having some startling or unreasonable consequence, such as overriding fundamental human rights, as not having been intended to do so. An intention to override such rights must be expressly stated or appear by necessary implication… Section 20(1) contained no express reference to legal professional privilege and the question is therefore whether its exclusion must necessarily be implied."
>
> (Id, paras. 7 and 8 of the opinion; emphasis added – H.M.)

In this context it should be further emphasized that there is a consensus that section 3 of the Communications Data Collection Act offers a more balanced arrangement in this respect, both substantively (the inclusion of detailed arrangements) and at the level of jurisdiction (the requirement that the application for the permit should be made to court, rather than the administrative authority.) The question is therefore whether, in view of the infringement to constitutional rights that underlie professional privilege, we can make do with a guideline that section 3 of the Communications Data Collection Act constitutes considerations (and nothing more) when exercising the power under section 4 of the Act. In my opinion, the answer to the question is in the negative. The overall proper constitutional result is therefore that the arrangement along the court "course" should constitute an exclusive mandatory course in the case of an application to obtain communications data concerning professionals. The reasons for this are explained below.

Professional Privilege Is Not to Be Infringed without a Judicial Order

20. Section 3 of the Communications Data Collection Act purports to also permit consideration of urgent cases (see: section 3(f)(2) of the Communications Data Collection Act, in the knowledge that the courts system is organized to respond to such situations 24 hours a day); the "course" prescribed in it is more balanced and proportional than that delineated in the "administrative course"; its infringement on such constitutional rights is less restrictive because it requires considering a greater range of factors. It furthermore requires the administrative authority to submit its justifications to judicial review. Given these factors, enabling the administrative authority "to circumvent" the balanced legal "course" in section 3 of the Communications Data Collection Act in the case of professionals is improper. As mentioned, a series of reasons support the above conclusion and they are set out immediately below.

21. The purpose of the professional privileges is to protect the constitutional values that justify them. They therefore cannot be infringed without suitable justification as provided in the Limitations Clause of Basic Law: Human Dignity and Liberty. Such justification is generally only possible through a judicial order, rather than administrative measures (*a fortiori* since the privileges are sometimes also presumed absolute.) This perception is what led to MKs Gideon Sa'ar and Shelly Yachimovich's proposal on second reading, in a reservation to the Act's Bill, the language of section 3(b) of the Act that was passed, providing as follows:

> "If the subscriber subject the motion is a professional, the court shall not allow communications data to be obtained as provided in subsection (a), unless it is satisfied, on the basis of clear details to such effect in the motion, that there are grounds to suspect that the professional is involved in the offense, in connection with which the motion was filed."

See: Knesset Proceedings of the 181st session of the 17th Knesset on December 17, 2007, at 12,895, 12,901.

These conditions strengthen the requirements the court faces when issuing an order to obtain communications data from the database of a telecommunications licensee, as set in section 3(a) of the Act, which mandate the court be satisfied that "it is necessary" for the purposes of the section "provided that obtaining the communications data does not infringe a person's privacy beyond necessary". We therefore have expression of the "Limitations Clause", which is to be applied in every specific motion and reviewed by the judicial authority. If it does not do so, a serious situation arises as stated by then MK Gideon Sa'ar:

> "… Whoever understands the significance in the relationship of attorney-client or journalistic privilege, or all those types of privilege, understands that it could be a device for suppressing all professional privilege" (id, at 12,895).

MK Shelly Yachimovich further refined matters in the context of journalistic privilege and stated:

> … And it could go further into somewhat darker realms, and the risk of leading to the unnecessary monitoring of a journalist's telephone lines might seriously impair his ability to function, the trust that his sources place in him, his ability to expose wrongdoing and corruption and therefore indirectly, or even directly, infringe the freedom of the press, which is a fundamental cornerstone of our democracy" (id, at 12,901)

22. In light of this, it appears to me that the approach that makes infringing professional privilege conditional upon obtaining a judicial order is the "proper constitutional" format, without which doing so is impossible. The language of section 52 of the Evidence Ordinance, which provides as follows, supports this as well:

> "The provisions of this chapter shall apply to providing evidence both to a court or tribunal and to any authority, body or person competent under law to hear evidence; and every reference in this chapter to a court shall be deemed to be a reference to a tribunal and to any such body or person as well."

In this regard, scholar Jacob Kedmi states in his work ON EVIDENCE, Part III (2009) as follows:

> "The prevailing approach is to view the term 'authority' as expressing the entities that are empowered <u>to conduct an investigation</u> within the meaning of <u>gathering evidence</u> (as distinct from other entities that are empowered <u>'to hear evidence'</u> in the way typical of giving testimony in court); and in that way to interpret the initial provision – as distinct from the final provisions that do not include the term 'authority' – as also applying to entities that are legally empowered 'to gather evidence,' like the Israel Police, income tax investigators, customs investigators, etc." (id, at 1012) (emphasis in original – H.M.).

This position was in fact adopted in CrimA 8600/03, *State of Israel v. Gilad Sharon*, IsrSC 58(1) 748 (2003), where an extended bench, per Deputy President T. Or, held as follows:

> "On its face, it may have been concluded that the Police, which collects evidence, could be treated as a 'court'… This result is unsatisfactory. It is unreasonable that the Police, in attempting to obtain certain documents and facing a suspect who asserts privilege, are charged with deciding whether he does indeed have privilege… Consequently, when a suspect being investigated by the Police claims a privilege applies, the Police investigator will not have power to decide whether the documents are privileged. In order to obtain the documents the investigator will have to request a court order" (id, at 766).

Here it should be stated that in MG, in Britain, a similar approach and interpretation were adopted.

It should further be noted that section 12 of the Communications Data Collection Act, which regulates the conflicts of laws, gives effect to this position, as follows:

> "The provisions of this Act shall not affect the powers granted by law in respect to obtaining information and documents, including communications data, but for a court's power under section 43 of the Criminal Procedure (Arrest and Search) Ordinance [New Version], 5729-1969 to order communications data to be presented or produced upon request by investigatory or prosecution authorities."

23. My above conclusion is further supported in terms of journalistic privilege – because of its special characteristics as discussed above since the interpretation expressed in the Police procedure and adopted by the President – does not *prima facie* bar that where a journalist is suspected of committing a felony (for example holding "secret information" within the meaning of section 113(c) of the Penal Law, 5737-1977) the authorities would seek to act in his regard according to section 4 of the Act or by another administrative method, and there have indeed been examples of this (see Nakdimon 274-276).

Moreover, in the analysis so far I have ignored the fact that the Police procedure's reference to the case of obtaining an "administrative permit" to gather communications data relating to a journalist is limited solely to traffic data (a list of incoming and outgoing calls) (see: section 7(b)(4) of the procedure). On its face this means there is no impediment to requesting other communications data, even when the journalist is not suspected of a "felony," but this is not expressed in the President's opinion. This is joined with the initial problem I have discussed above, and even aggravates it, because other communications data can also infringe the journalist's privilege to the same extent as traffic data. For example, location data regarding communications equipment in the journalist's possession could expose or help to expose the source of the privileged information (on the distinction between location data and traffic data, see: section 1 of the Communications Data Collection Act.) In this respect Nakdimon states as follows:

> "It appears to me that this state of affairs, where journalistic privilege as to communications data is partly regulated by internal Police directives – that might change from time to time otherwise than in the context of public proceedings, and from which the authority might depart – rather than principal legislation, is improper. Moreover, the substance of the arrangement prescribed in the directives is also inadequate because it leaves the door open to circumventing journalistic privilege, without judicial review that would facilitate its protection where it is asserted that the journalist is suspected of the offense involved in the investigation or is its victim, or when the communications data sought are not traffic data but, for example, location data that enable knowing exactly where the

parties to the communication between the journalist and the source of information are" (see: id, at 277; emphasis added – H.M.).

This logical statement is apt here and it appears to me that it also appropriately sums up my overall position. The time has therefore come to conclude the matter.

Conclusion

24. In conclusion, in light of the Communication Data Collection Act's potential significant infringement on professionals' privilege and their protected constitutional rights, I believe that the scope of the Act should be confined by an interpretive determination that the "administrative course" to obtain a permit may not be used where the permit is sought regarding professional privilege. In such a case, the "legal course" will in my opinion constitute an exhaustive and exclusive arrangement. Furthermore – again in the scope thereof – a court would grant an order for disclosure only when the conditions of the "Limitations Clause" were met and when the court is satisfied, in the context of the "professional privilege," that the interest of collecting the data outweighs the constitutional values that justify the specific privilege.

25. A review of the history that has recognized professional privilege – in Israel and elsewhere in the world – demonstrates that individual rights were developed and founded, *inter alia*, on the basis of this specific area of law. This was the case in the past and although the present is somewhat complex, as noted, I trust this will also be the case in the future given the need to contend with the challenges with which new technology, the Act and the case law present us.

Deputy President E. Rivlin

I join in the result my colleague President D. Beinisch reached, whereby the petitions should be rejected, in light of and subject to the boundaries and limitations detailed in the judgement.

My colleague Justice H. Melcer rightly insists on the need for special protection the Act should afford anyone with professional privilege under statute or case law. He believes that a competent officer should not be permitted to act under section 4 of the Act where privilege *prima facie* applies because of a profession and that the only way to obtain communications data in those situations must be approaching a court.

As for myself, I would not go so far as to rule out the administrative course in those cases. Nevertheless, I do agree that extreme care should be taken in such cases, as reflected in my colleagues the President and Justice E. Arbel's opinions. First, as President D. Beinisch held regarding exercising the power in both section 3 and section 4 of the Act, it should be interpreted so that the data is only obtained where it is required for a specific, concrete need. Second, regarding the exercise of the power in section 4 of the Act, it should be interpreted, as she proposed, so that it is used sparingly in extreme cases for the purpose of dealing with offenses that require it and

only where because of the urgency it is impossible to obtain a court order; this is when the motive for applying to court is a serious circumstance such as a risk to human life. The fact that the subscriber is a professional person should also be taken into account when exercising the power under section 4 or refraining from doing so.

As my colleague Justice E. Arbel believes, I too believe that section 4 of the Act should be construed to preclude the competent officer's authority to renew a permit. After issuing the initial permit, which is not to exceed 24 hours, section 4 should be interpreted so that the permit may only be renewed by a court.

Unanimously decided to dismiss the petitions.

Regarding the interpretation of sections 3, 6 and 7 of the Act, it is decided according to President (Ret.) D. Beinisch's opinion, joined by all members of the bench.

Regarding the interpretation of section 4 of the Act, it is decided by a majority of the bench, as stated in President (Ret.) D. Beinisch's opinion, that the power can also be exercised where the communications data are sought from a "professional," always subject to the limitations and reservations detailed in the opinion. This is against Justice H. Melcer's dissenting opinion, who believes that the power prescribed in section 4 may not be exercised in order to obtain a permit under the Law in the case of a "professional".

May 28, 2012 (7th Sivan 5772)