Protection of Privacy Law, 5741 – 1981[1]

Chapter One: Infringement of Privacy

Prohibition of infringement of privacy

1. No person shall infringe the privacy of another without his consent.

What is infringement of privacy

2. Infringement of privacy is any of the following:

(1) spying on or trailing a person in a manner likely to harass him, or any other harassment;

(2) listening-in prohibited under any Law;

(3) photographing a person while he is in the private domain;

(4) publishing a person's photograph under such circumstances that the publication is likely to humiliate him or bring him into contempt;

(5) copying or using, without permission from the addressee or writer, the contents of a letter or any other writing not intended for publication, unless the writing is of historical value or fifteen years have passed since the time of writing. In this section "writing" - including electronic message as defined in Electronic Signature Law, 5761 – 2001.

(6) using a person's name, appellation, picture or voice for profit;

(7) infringing a duty of secrecy laid down by law in respect of a person's private affairs;

(8) infringing a duty of secrecy laid down by express or implicit agreement in respect of a person's private affairs;

(9) using, or passing on to another, information on a person's private affairs otherwise than for the purpose for which it was given;

(10) publishing or delivering anything obtained by way of an infringement of privacy under paragraphs (1) to (7) or (9);

(11) publishing any matter relating to a person's intimate life, including his sexual history, state of health or conduct in the private domain.

[1] This translation is based on the official translation of the law as published in 1981. Later amendments of the law were not officially translated.

Definition of terms

3. In this Law -

"person", for the purposes of sections 2, 7, 13, 14, 17B, 17C, 17F, 17G, 23A, 23B and 25, does not include a body corporate;

"consent" means informed, express or implied consent;

"possessor, for the purpose of a database" means a person who has a database in his possession permanently and is permitted to use it;

"publication" has the same meaning as in section 2 of the Prohibition of Defamation Law, 5725-1965;

"photography" includes filming;

"use" includes disclosure, transfer and delivery.

Infringement of privacy a civil wrong

4. An infringement of privacy is a civil wrong, and the provisions of the Civil Wrongs Ordinance (New Version) shall apply to it subject to the provisions of this Law.

Infringement of privacy an offense

5. A person who willfully infringes the privacy of another in any of the ways stated in sections 2(1), (3) to (7) and (9) to (11) is liable to imprisonment for a term of five years.

Trifling act

6. No right to bring a civil or criminal action under this Law shall accrue though an infringement of no real significance.

Chapter Two: Protection of Privacy in Database

Definitions

7. In this chapter –

"information security" means protection of the integrity of the information, or protection of the information from being exposed, used or copied, without lawful permission;

"database" means a collection of data, kept by a magnetic or optic means and intended for computer processing, except –

(1) a collection for personal use that is not for business purposes; or

(2) a collection that includes only the name, address and method of communication, which in itself does not produce a characterization which infringes the privacy of the persons whose names are included therein,

provided that the owner of the collection or the body corporate under his control does not have another collection;

"information" means data on the personality, personal status, intimate affairs, state of health, economic position, vocational qualifications, opinions and beliefs of a person;

"sensitive information" means -

(1) data on the personality, intimate affairs, state of health, economic position, opinions and beliefs of a person;

(2) information that the Minister of Justice determined by order, with the approval of the Constitution, Law and Justice Committee of the Knesset, is sensitive information;

"manager of database" means an active manager of a body that owns or possesses a database or a person whom the aforesaid manager authorized for this purpose;

"Registrar" means a person who has the qualifications to be appointed judge of a Magistrate's Court, and was appointed by the Government, by notice in *Reshumot*, to keep a "Register of Databases" (hereinafter referred to as "the Register") as prescribed in section 12;

"information integrity" means the data in the database is identical to the source from which it was drawn, not having been changed, delivered or destroyed without lawful permission.

Part One: Databases

Registration and use of database

8. (a) No person shall manage or possess a database that requires registration pursuant to this section, unless one of the following has occurred:

(1) the database has been registered in the Register;

(2) an application has been made to register the database and the provisions of section 10(B1) have been met;

(3) the database requires registration pursuant to subsection (e) and the Registrar's order permitted management and possession of the database until the time of its registration.

(b) A person shall not use information in a database that requires registration under this section except for the purpose for which the database was established.

(c) A database owner is obligated to register his database in the Registry, and he shall register the database if one of the following applies:

(1) the database contains information on more than 10,000 persons;

(2) the database contains sensitive information;

(3) the database includes information on persons, and the information was not delivered to this database by them, on their behalf or with their consent to this database;

(4) the database belongs to a public body as defined in section 23;

(5) the database is used for direct-mailing services as referred to in section 17C.

(d) The provisions of subsection (c) shall not apply to a database that only contains information that was made public pursuant to lawful authority or was made available for public inspection pursuant to lawful authority;

(e) The Registrar may, for special reasons that shall be recorded, order the registration of a database that is exempt from registration pursuant to subsections (c) and (d); the said order, in which the Registrar shall set forth instructions as to managing and possessing the database until its registration, shall be served to the owner of the database.

Application for registration

9. (a) An application for registration of a database shall be submitted to the Registrar.

(b) An application for registration shall state –

(1) the names of the owner of the database, the possessor of the database and the manager of the database, and their addresses in Israel;

(2) the purposes for which the database was established and the purposes for which the information is intended;

(3) the kinds of information that will be included in the database;

(4) particulars on the transfer of information abroad;

(5) particulars on receiving information, on a permanent basis, from a public body as defined in section 23, the name of the public body delivering the information and the nature of the information delivered, except for particulars that are delivered with the consent of the persons as to whom the information relates.

(c) The Minister of Justice may prescribe by regulations further particulars to be stated in the application for registration.

(d) The owner or possessor of a database shall notify the Registrar of every change in any of the particulars specified in subsection (b) or in subsection (c) and of the discontinuance of the operation of the database.

Powers of Registrar

10. (a) Where an application for registration of a database is submitted –

(1) The Registrar shall register it in the register it, within 90 days from the day the application was submitted to him, unless he sees reasonable cause for believing that the database serves or is liable to serve illegal activities or as a cover for them, or that the information included within it was received, accumulated or collected in violation of this Law or in violation of the provisions of any law;

(2) The Registrar may, if he is of the opinion doing so is appropriate for the actual operation of the database, record a different purpose than the one set forth in the application, record a number of purposes for the database, or order the submission of a number of applications under the application that was submitted;

(3) The Registrar shall not refuse to register the database pursuant to paragraph (1) and shall not exercise his powers pursuant to paragraph (2) unless he has given the applicant an opportunity to be heard.

(b) Repealed.

(b1) Where the Registrar does not register the database within 90 days from the day the application was submitted to him, and does not notify the applicant of his refusal to register or of delay of the registration for special reasons that he shall record in his notice, the applicant may manage or possess the database although it is not registered.

(b2) Where the Registrar notifies the applicant of his refusal to register the database or of delaying the registration as stated in subsection (b1), the applicant shall not be allowed to manage or possess the database, unless the court rules otherwise.

(b3) The Registrar shall delete the registration of a database from the Register if the owner of the database notifies him that the information in the database has been destroyed and verified the notice by affidavit; where a person other than the owner possesses the database, the notice shall also be

verified by affidavit of the possessor.

(c) The Registrar shall supervise compliance with the provisions of this Law and the regulations thereunder.

(d) The Minister of Justice, with the approval of the Constitution, Law and Justice Committee of the Knesset, shall establish by order, a supervisory unit that will supervise the databases, their registration, and the information security therein; the unit shall be sized accordingly with the supervision needs.

(e) The Registrar shall head the supervisory unit, and shall appoint inspectors to carry out the supervision pursuant to this Law; no person shall be appointed inspector unless he received the appropriate professional training in the field of computerization and information security and exercising powers under this Law, and the Israel Police did not object to his appointment for reasons of public safety.

(e1) In carrying out his functions, an inspector may –

(1) demand every relevant person to deliver to him information and documents relating to a database;

(2) enter a place as to which he has reasonable belief that a database is being operated, search the place and seize objects, if he is convinced that doing so is necessary to ensure implementation of this Law and to prevent violation of its provisions; the provisions of the Criminal Procedure (Arrest and Search) Ordinance [New Version], 5869 – 1969 shall apply to an object that has been seized under this section; arrangements for entering a military installation or an installation of a security authority within its meaning in section 19(c) shall be determined by the Minister of Justice upon consultation with the minister in charge of the security authority, as the case may be; in this paragraph, "object" includes computer material and output as defined in the Computers Law, 5765 – 1995;

(3) notwithstanding the provisions of paragraph (2), an inspector shall not enter a place that is used solely as a residence, other than pursuant to an order given by a judge of the Magistrate's Court.

(f) Where the possessor or owner of a database infringes any provision of this Law or the regulations thereunder, or fails to comply with a request made to him by the Registrar, the Registrar may suspend the registration for a period that he shall determine or cancel the registration of the database in the Register, provided that prior to the suspension or cancellation the owner of the database was given the opportunity to be heard.

(g) The Registrar and any person acting on his behalf shall be treated as State employees.

Protection of privacy report

10A. No later than the first of April every year, the Protection of Privacy Council shall submit to the Constitution, Law and Justice Committee of the Knesset a report that the Registrar shall prepare on the enforcement and supervisory activities in the year preceding submission of the report, along with the Council's comments.

Notice to accompany request for information

11. A request to a person for information with a view to the keeping and use thereof in a database shall be accompanied by a notice indicating –

(1) whether that person is under a legal duty to deliver that information or whether its delivery depends on his volition and consent;

(2) the purpose for which the information is requested;

(3) to whom the information is to be delivered and the purposes of such delivery.

Register of databases

12. (a) The Registrar shall keep a register of databases, which shall be open for inspection by the public.

(b) The register shall contain the particulars for registering the database as stated in section 9.

(c) Notwithstanding the provisions of subsections (a) and (b), in a database of a security authority, the particulars stated in section 9(b)(3), (4) and (5) shall not be open to inspection by the public.

Right to inspect information

13. (a) Every person is entitled to inspect, either himself or through a representative authorized by him in writing or his guardian, any information about him kept in a database.

(b) The owner of a database shall enable, at the request of a person referred to in subsection (a) (hereinafter – person making the request) inspection of the information, in the Hebrew, Arabic or English language.

(c) The owner of a database may refuse to deliver to the person making the request information relating to his physical or mental health if, in his opinion, it is liable to severely harm the physical or mental health of the person making the request or endanger his life; in such case, the owner of the database shall deliver the information to a physician or

psychologist on behalf of the person making the request.

(c1) The provisions of this section shall not require the delivery of information in violation of a privilege prescribed by law, unless the person making the request is the person who is the beneficiary of the privilege.

In this subsection, "law" includes common law.

(c2) The mode and conditions of, and the payment for, the exercise of the right of inspection of information shall be prescribed by regulations.

(c3) The provisions of this section shall not apply –

(1) to a database of a security authority within the meaning of section 19(c);

(1A) to a database of the Prisons Service;

(2) to a database of a tax authority within the meaning of the Tax Law Amendment (Exchange of Information between Tax Authorities) Law, 5727 – 1967;

(3) where the security or foreign relations of the State or the provisions of any enactment require that information about any person not be disclosed to him;

(4) to any database, in respect of which the Minister of Justice, in consultation with the Minister of Defense or the Minister of Foreign Affairs, as the case may be, and with the approval of the Foreign Affairs and Security Committee of the Knesset, has determined that it contains information as to which the security or foreign relations of the State requires or require that it not be disclosed (such information hereinafter referred to as "secret information"), provided that a person wishing to inspect information about himself kept at any such database shall be entitled to inspect information other than secret information.

(5) to a database about investigations and law enforcement of an authority empowered to investigate by law an offense, which the Minister of Justice determined by order, with the approval of the Constitution, Law and Justice Committee of the Knesset.

(6) to a data base established under section 28 of the Prohibition on Money Laundering Law, 5760 –2000.

Inspection of information not in the possession of the

13A. Without derogating from the provisions of section 13 –

(1) The owner of a database who keeps it at the place of another person (in this section - the possessor) shall refer

owner of the database

the person making the request to the possessor, with his address, and order the possessor, in writing, to enable the person making the request the inspection;

(2) Where the person making the request applies to the possessor first, the possessor shall inform him if he possesses information about him, and also the name and address of the owner of the database.

Amendment of information

14. (a) A person who, on inspecting any information about himself finds that it is not correct, not complete, not clear or not up to date may request the owner of the database or, if such owner is a non-resident, the possessor thereof to amend or delete the information.

(b) Where the owner of a database agrees to a request under subsection (a), he shall make the necessary changes in the information and shall notify them to every person who received the information from him within a period prescribed by regulations.

(c) Where the owner of a database refuses to comply with a request under subsection (a), he shall give notice to such effect, in the form and manner prescribed by regulations, to the person who made the request.

(d) The possessor is obligated to correct the information, if the owner of the database agreed to the requested correction or the court ordered that the correction be made.

Appeal to court

15. A person requesting information may, in the form and manner prescribed by regulations, appeal to the Magistrate's Court against refusal by the owner of a database to enable inspection under section 13 or section 13A and against notice of refusal under section 14(c).

Secrecy

16. No person shall disclose any information obtained by him by virtue of his functions as an employee, manager or possessor of a database save for the purpose of carrying out his work or implementing the Law or under a court order in connection with a legal proceeding; where the request is made before a proceeding has been instituted, it shall be heard in the Magistrate's Court.

A person who infringes the provisions of this section shall be liable to imprisonment for a term of five years.

Responsibility to

17. A database owner, possessor or manager, are each responsible

information security — for the information security in the database.

Possessor of databases of different owners

17A. (a) A person who possesses databases of different owners shall ensure that access to each database is provided only to persons who are expressly authorized to do so by written agreement between the person and the owner of the said database.

(b) A person who possesses at least five databases that require registration under section 8 shall deliver annually to the Registrar a list of the databases in his possession, indicating the names of the owners of the databases, verified by affidavit that, in respect of each of the databases, the persons entitled to access to the database were determined by agreement between the person and the owner, and the name of the security supervisor, as referred to in section 17B.

Security supervisor

17B. (a) The bodies set forth below shall appoint a person with the appropriate qualifications to be in charge of the information security (hereinafter – security supervisor):

(1) a possessor of five databases that require registration under section 8;

(2) a public body as defined in section 23;

(3) a bank, an insurance company, a company involved in rating or evaluating credit.

(b) Without derogating from the provisions of section 17, the security supervisor shall be responsible for the information security in the databases kept in the possession of the bodies referred to in subsection (a)

(c) A person who has been convicted of an offense involving moral turpitude or an offense of the provisions of this Law shall not be appointed as security supervisor.

Part Two: Direct Mailing

Definitions

17C. In this part –

"direct mailing" means contacting a person personally, based on his belonging to a group of the population that is determined by one or more characteristics of persons whose names are included in a database;

"contact" includes in writing, printed matter, telephone, facsimile, in a computerized way or by other means;

"direct-mailing services" means providing direct-mailing

services to others by way of transferring lists, labels or data by any means.

Direct mailing

17D. A person shall not manage or possess a database used for direct-mailing services, unless it is registered in the Register and one of its registered purposes is mailing services.

Mentioning source of the information

17E. A person shall not manage or possess a database used for direct-mailing services, unless he has a record indicating the source from which he received every collection of data used for the database, and the date it was received, and to whom each said collection of data was delivered.

Deletion of information from a database used for direct mailing

17F. (a) Every contact by direct mailing shall include in a clear an conspicuous manner –

(1) mention that the contact is direct mailing, indicating the registration number of the database being used for direct-mailing services as stated in the Register of databases;

(2) notice of the right of the recipient of the contact to be removed from the database as referred to in subsection (b); along with the address which he should contact for this purpose;

(3) the name and address of the owner of the database containing the information based on which the contact was made, and the sources from which the owner of the database received this information.

(b) Every person is entitled to demand, in writing, of the owner of the database used for direct mailing that the information relating to him be deleted from the database.

(c) Every person is entitled to demand, in writing, of the owner of the database used for direct-mailing services or of the owner of the database containing the information based on which the contact was made, that the information relating to him not be delivered to a person, to a type of persons or to specific persons, for either a limited period of time or permanently.

(d) Where a person informed the owner of the database of his demand as specified in subsections (b) or (c), the owner of the database shall act in accordance with the demand and notify the person, in writing, that he acted accordingly.

(e) Where the owner of the database did not give notice as specified in subsection (d) within 30 days from the day of

receipt of the demand, the person whom the information is about may apply to the Magistrate's Court in the manner prescribed by regulations, to order the owner of the database to act as specified.

(f) The rights under this section of a deceased person recorded in a database are given also to his spouse, child, parent or sibling.

Application to data items

17G. The provisions of this part shall apply to data items relating to the private affairs of a person, although not classified as information, in the same way that they apply to information.

Non-application to a public body

17H. This part shall not apply to a public body within the meaning of section 23(1) in carrying out its functions under law.

Saving of laws

17I. The provisions of this part are in addition to the provisions of any law.

Chapter Three: Defenses

Defenses

18. In any criminal or civil proceeding for infringement of privacy, it shall be a good defense if one of the following is the case:

(1) the infringement was committed by way of a publication protected under section 13 of the Defamation (Protection) Law, 5725 – 1965;

(2) the defendant or accused committed the infringement in good faith and in any of the following circumstances:

(a) he did not know and need not have known that an infringement of privacy might occur;

(b) the infringement was committed in circumstances in which the infringer was under a legal, moral, social or professional obligation to commit it;

(c) the infringement was committed in defense of a legitimate personal interest of the infringer;

(d) the infringement was committed in the lawful pursuit of the infringer's occupation and in the ordinary course of his work, so long as it was not committed by way of publication;

(e) the infringement was committed by way of taking a photograph, or of publishing a photograph taken, in the public domain, and the injured party appears in it

accidentally;

(f) the infringement was committed by way of a publication protected under paragraphs (4) to (11) of section 15 of the Defamation (Prohibition) Law, 5725 – 1965;

(3) The infringement involved a public interest justifying it in the circumstances of the case, provided that, if the infringement was committed by way of publication, the publication was not untruthful.

Exemption

19. (a) No person shall bear responsibility under this Law for an act which he is empowered to do by law.

(b) A security authority or a person employed by it or acting on its behalf shall bear no responsibility under this Law for an infringement reasonably committed within the scope of their functions and for the purpose of carrying them out.

(c) For the purposes of this section, "security authority" means any of the following:

(1) the Israel Police;

(2) the Intelligence Branch of the General Staff, and the Military Police, of the Israel Defense Forces;

(3) the General Security Service;

(4) the Intelligence and Special Duties Agency (Mossad).

Onus of proof

20. (a) Where the accused or defendant proves that he committed infringement of privacy under any of the circumstances referred to in section 18(2) and that it did not exceed the limits reasonable under those circumstances, he shall be presumed to have committed it in good faith.

(b) The accused or defendant shall be presumed not to have committed the infringement of privacy in good faith if in committing it he knowingly went further than was reasonably necessary for the purposes of the matters protected by section 18(2).

(c) An accused person or defendant who sets up the plea provided by section 18(2)(b) or (d) shall be presumed not to have infringed privacy in good faith if he infringed it in violation of the rules or principles of professional ethics applying to him by law or accepted by members of the profession to which he belongs; however, this presumption will not apply if the infringement was caused in circumstances that the accused person or defendant acted according to a legal duty that was imposed on him.

Rebuttal of defense pleas

21. Where the accused or defendant produces evidence or himself testifies to prove one of the defense pleas provided by this Law, the prosecutor or plaintiff may produce rebutting evidence. This provision shall not derogate from the power of the court under any law to permit the production of evidence by the parties.

Mitigating circumstances

22. In passing sentence or awarding compensation, the court may also take the following into account in favor of the accused or defendant:

(1) that the infringement of privacy was merely a repetition of something said before and that he mentioned the source on which he relied;

(2) that he did not intend to commit an infringement;

(3) if the infringement was committed by way of publication – that he has apologized and has taken steps for the discontinuance of the sale or distribution of copies of the publication containing the infringement, provided that the apology was published in the same place and in the same dimensions and manner in which the infringing matter had been published and was unqualified.

Chapter Four: Imparting of Information or Data Items by Public Bodies

Definitions

23. In this chapter –

"public body" means

(1) a Government Department and any other State institution, a local authority and any other body carrying out public functions under any law;

(2) a body designated by the Minister of Justice, by order, with the approval of the Constitution, Law and Justice Committee of the Knesset, provided that the order shall prescribe the categories of information and data items which the body may impart and receive.

Application to any data items

23A. The provisions of this chapter shall apply to any data items as to a person's private affairs, even though it may not come within the definition of information, in like manner as they apply to information.

Prohibition of

23B. (a) The imparting of information by a public body is prohibited

delivery of information

unless it has been published by lawful authority, or the person to whom it relates has consented to its being imparted.

(b) The provisions of this section shall not prevent a security authority, within the meaning of section 19, from receiving or imparting information for the purpose of carrying out its functions, provided that its communication or receipt is not prohibited by any enactment.

Restriction as to prohibition

23C. Notwithstanding the provisions of section 23B, the imparting of information, unless prohibited by any enactment or by the principles of professional ethics, is permitted –

(1) between public bodies if –

(a) the imparting of the information takes place within the framework of the powers or functions of the person imparting the information and is required for the purpose of implementing any enactment or for any purpose within the framework of the powers or functions of the person importing or receiving the information, or

(b) the information is imparted to a public body permitted by law to demand it from any other source;

(2) from a public body to a Government Department or other State institution, or between such Departments or institutions as aforesaid, if the imparting of the information is required for the purpose of implementing any enactment or for any purpose within the framework of the powers or functions of the person imparting or receiving the information; provided that no information shall be imparted as aforesaid if it had been given on condition that it not be communicated to another.

Duties of public body

23D. (a) A public body which regularly imparts information under section 23C shall indicate such fact in every request for information made in accordance with the Law.

(b) A public body which imparts information under section 23C shall keep a record of the information imparted.

(c) Where a public body receives information under section 23C and such information is stored in a database, it shall notify the Registrar of such fact, and such fact shall be included in the particulars of the list of databases under section 12.

(d) A public body which receives information under section 23C shall only make use of it within the framework of its

powers or functions.

(e) For the purposes of the duty of secrecy under any law, any information communicated to a public body by virtue of this Law shall be treated like information obtained by that body from any other sources and, in addition, all the provisions applying to the communicating body shall apply to the receiving body.

Excess information

23E. (a) Where any information permitted to be imparted under sections 23B or 23C is stored in a file with any other information (hereinafter referred to as "excess information"), the communicating body may deliver to the receiving body such first-mentioned information together with the excess information.

(b) Excess information may only be imparted under subsection (a) if procedures have been prescribed preventing any use being made thereof. Such procedures shall be prescribed by regulations. So long as they have not been so prescribed, the requesting body shall prescribe procedures in writing and shall forward a copy thereof to the communicating body upon its request.

Permitted delivery is not an infringement of privacy

23F. The imparting of information permitted under this Law shall not constitute an infringement of privacy and the provisions of sections 2 and 8 shall not apply thereto.

Regulations

23G. The Minister of Justice may, with the approval of the Constitution, Law and Justice Committee of the Knesset, make regulations as to procedure for the imparting of information by public bodies.

Penalties

23H. Repealed.

Chapter Five: Miscellaneous

Status of the State

24. This Law shall apply to the State.

Death of injured party

25. (a) Where a person whose privacy has been infringed dies within six months after the infringement without having filed an action or complaint in respect thereof, his spouse, child or parent or, if he leaves no spouse, child or parent, his brother or sister may file an action or complaint in respect of

that infringement within six months after his death.

(b) Where a person who has filed an action or complaint in respect of an infringement of privacy dies before the termination of the proceeding, his spouse, child or parent or, if he leaves no spouse, child or parent, his brother or sister may, within six months after his death, notify the court that he or she wishes to proceed with the action or complaint, and upon so notifying, he or she shall take the place of the plaintiff or complainant.

Prescription

26. The period of prescription of civil actions under this Law is two years.

Applicability of certain provisions of the Prohibition of Defamation Law.

27. The provisions of sections 21, 23 and 24 of the Defamation (Prohibition) Law, 5725 – 1965, shall apply *mutatis mutandis* to legal proceedings for infringement of privacy.

Evidence as to person's bad reputation, character or past

28. In a criminal or civil proceeding for infringement of privacy, no evidence shall be produced, and no witness shall be examined, as to the bad reputation or as to the character, past, activities or opinions of the injured party.

Additional orders

29. (a) In addition to any penalty and other relief, the court may, in a criminal or civil proceeding for infringement due to a violation of a provision of this law, order –

(1) prohibition of the distribution of copies, or confiscation, of the infringing matter; a confiscation order under this paragraph is effective against any person who has such material in his possession for sale, distribution or storage, also if he is not a party to the proceeding; where the court orders confiscation, it shall direct how the confiscated copies shall be disposed of;

(2) publication of the whole or part of the judgment; the publication shall be made at the expense of the accused or defendant, in the place and in the dimensions and manner prescribed by the court.

(3) surrender of the infringing matter to the injured party;

(4) destruction of information unlawfully received, or prohibition of use of the aforesaid information or of excess information as defined in section 23E, or any

other order in respect of the information.

(b) The provisions of this section shall not prevent the keeping of a copy of a publication in public libraries, archives and the like unless the court, by a confiscation order under subsection (a)(1), imposes a restriction also on such keeping, and they shall not prevent the keeping of a copy of a publication by an individual.

Statutory damages

29A. (a) The court may order a person who has been convicted under section 5 to pay the injured person statutory damages, that will not exceed 50,000 new shekels; an order for damages under this subsection shall be regarded as a ruling of the same court in a civil proceeding of the entitled against the person obliged.

(b) (1) In a civil wrong-doing proceeding under section 4, the court may order that the defendant shall pay the plaintiff statutory damages that will not exceed 50,000 new shekels.

(2) In a proceeding under paragraph (1) in which it was proven that the infringement on privacy was made with intent to cause harm, the court may order that the defendant shall pay the plaintiff statutory damages that will not exceed double the amount in that paragraph.

(c) A person shall not be awarded statutory damages under this section, for the same infringement on privacy, more than once.

(d) The amounts in this section shall be updated at the 16th of each month, in accordance with the rate of change in the new index compared with the basic index; in this regard-

"index" – the consumer price index as published by the Centeal Bureau of Statistics;

"the new index" – the index of the month which proceeded the month of update;

"the basic index" – the index of May 2007.

Responsibility for publication in newspaper

30. (a) Where an infringement of privacy is published in a newspaper, within the meaning of the Press Ordinance (hereinafter referred to as "a newspaper"), criminal and civil responsibility for the infringement shall be borne by the person who brought the material to the newspaper and thereby caused its publication, the editor of the newspaper and the person who actually decided upon the publication of the infringement in the newspaper, and civil responsibility shall be borne also by the publisher of the newspaper.

(b) In a criminal case under this section, it shall be a good defense for the editor of the newspaper that he took reasonable steps to prevent the publication of the infringement or that he did not know of the publication.

(c) In this section, "editor" of a newspaper includes the actual editor.

Penalty for offenses of strict responsibility

31A. (a) A person who commits any of the following is subject to imprisonment for a term of one year –

(1) manages, possesses or uses a database in violation of the provisions of section 8;

(2) provides incorrect particulars in an application for registration of a database as required in section 9;

(3) fails to provide particulars or provides incorrect particulars in the notice accompanying a request to obtain information under section 11;

(4) fails to comply with the provisions of sections 13 and 13A regarding the right to inspect information kept in a database or fails to correct information in accordance with the provisions of section 14;

(5) enables access to a database in violation of the provisions of section 17A(a) or fails to provide to the Registrar documents or an affidavit in accordance with the provisions of section 17A(b);

(6) fails to appoint a security supervisor in accordance with the provisions of section 17B;

(7) manages or possesses a database used for direct-mailing services, in violation of the provisions of sections 17D to 17F;

(8) delivers information in violation of the provisions of sections 23B to 23E.

(b) An offence under this section does not require proof of criminal intent or negligence.

Civil wrong

31B. An act or omission in violation of the provisions of chapters two or four or in violation of regulations enacted under this Law shall be a wrong under the Civil Wrongs Ordinance [New Version].

Responsibility of printer and distributor

31. Where an infringement of privacy is published in print, except in a newspaper published under a valid license at intervals of not less than forty days, criminal and civil responsibility for the infringement shall be borne also by the possessor of the printing

press, within the meaning of the Press Ordinance, in which the infringement was printed and by a person who sells or otherwise distributes the publication; provided that they shall not bear responsibility unless they knew or ought to have known that the publication contained an infringement of privacy.

Material inadmissible as evidence

32. Material obtained by the commission of 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 it to be used or if the infringer, being a party to the proceeding, has a defense or enjoys exemption under this Law.

Amendment of Civil Wrongs Ordinance

33. Section 34A of the Civil Wrongs Ordinance [New Version] is hereby repealed.

Amendment of Criminal Procedure Law

34. In the schedule to the Criminal Procedure Law, 5725 – 1965, the following paragraph shall be added after paragraph (12):

"(13) offenses under the Protection of Privacy Law, 5741 – 1981."

Saving of laws

35. The provisions of this Law shall not derogate from the provisions of any other law.

Implementation of regulations

36. The Minister of Justice is charged with the implementation of this Law and may, with the approval of the Constitution, Law and Justice Committee of the Knesset, make regulations as to any matter relating to its implementation, and *inter alia* –

(1) conditions of keeping and safeguarding information at databases;

(2) conditions of transmitting information to or from databases outside the boundaries of the State;

(3) rules of conduct and ethics for owners, possessors and managers of databases and their employees.

Fees

36A. (a) The Minister of Justice, with the approval of the Constitution, Law and Justice Committee of the Knesset, may institute –

(1) fees for registration of a database and its inspection under this Law;

(2) a fee, for a period that shall be determined, for a

database registered in the Register (hereinafter – periodic fee), unless the database is owned by the State, in addition, the Minister may fix different amounts for the periodic fee, based on the kind of database, and also fix the date on which the period fees shall be paid, and an additional fee for a periodic fee that is not paid at the fixed time.

(b) The funds collected from the fees under this section shall be designated for the Registrar and the supervisory unit for purposes of carrying out their activities under this Law.

(c) Where the periodic fee or the additional fee to the periodic fee is not paid, as the case may be, within six months from the date fixed by regulations for payment of the additional fee, the registration of the database in the Register shall be suspended until payment is made.

Commencement

37. Chapter Two shall come into force six months from the date of publication of this Law.