PRIVACY LAWS & BUSINESS
DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

INTERNATIONAL newsletter

ISSUE NO 64 SEPTEMBER 2002

in this issue

Editorial

This newsletter follows the successful 15th PL&B Annual International Conference in Cambridge. Participants replenished their intellectual stores and, perhaps equally important, enjoyed the chance to share ideas with informed colleagues in the fine atmosphere of Cambridge. Conference reports highlight perspectives from the European Commission and France (p.9-11), and organisations such as the Royal Bank of Canada (p.6) and Microsoft (p.16).

Two privacy staples – spam and cookies - continue in some cases to annoy and, in other cases, to raise thorny legal issues (p.19-21). "Spam" continues to be the unwelcome "guest" on various modes of communications, from e-mail to mobile phones. Organisations outside the EU that make use of cookies may find their activities falling within the jurisdiction of the EU Data Protection Directive (p.12).

We also report on how several Asian countries are monitoring e-mail and Internet activity in an attempt to censor communications and information flows (p.21). At the same time, organisations in Europe and the United States face obligations to retain Internet data traffic, and Finnish ISPs may soon be obliged to monitor the websites they host for hate messages (p.24).

Internet and computer network security concerns surface in several articles. Allegedly security-conscious governments still manage to lose scores, if not hundreds, of laptop computers (p.4-5). Other governments struggle with massive fraud in the issue of the "breeder" documents that form the basis of many prospective schemes for authenticating the identity of individuals (p.4). Almost in the same breath, the OECD issues new guidelines emphasising the need for a "culture of security" around information systems (p.18).

Eugene Oscapella, Associate Editor
PRIVACY LAWS & BUSINESS

Israel's data protection law provides European level rights and duties

By Naomi Assia

NAOMI ASSIA TAKES A DETAILED LOOK at how European-style comprehensive data protection and privacy legislation has been developed in Israel over the last 20 years. Amendments made in 2000 cover transfers of personal data from Israel.

THE CONSTITUTIONAL RIGHT TO PRIVACY IN ISRAEL

The right to privacy in Israel gained constitutional status with the adoption of the 1992 Basic Law: Human Dignity and Freedom, (the "Basic Law"). Section 7(a) of the Basic Law provides that every person is entitled to privacy. Section 7(d) states that this privacy applies to conversations, writings and documents.

THE PROTECTION OF PRIVACY LAW – 1981

The law that provides the principles and details regarding the protection of privacy in Israel is the Protection of Privacy Law – 1981 (the "Law") which was enacted before the Basic Law. The Law protects individuals, but not corporations. Section 1 of the Law prohibits any violation of the privacy of others without consent. Many other laws contain explicit reference to the protection of data in a similar way to the Protection of Privacy Law. However, these laws address specific issues, and do not state a general right to privacy.

Section 2 of the Law lists the actions which, if conducted without consent, constitute a "violation of privacy." These include using, or passing on to another, information on a person's private affairs, otherwise than for the purpose for which it was given" and "publishing or passing on anything that was obtained by the way of violation of privacy."

In addition to the general right of privacy, chapters B and D ensure the privacy of databases. These chapters were originally enacted in 1981. However, because of the enormous progress in technology, they soon become outdated and were replaced in 1996, by Amendment no.4 (Databases) – 1996 (the "Amendment"). The Amendment's main purpose was to adjust chapter B to the new reality of the information market.

Prior to the Amendment, the term "database" was so broad that almost every computer holding data on individuals was considered a database. Such databases had to be recorded in the official list of databases, and neglecting to do so was a criminal offence.

The Amendment helped resolve this problem by narrowing the scope of the term "database" and by requiring registration only for certain databases. "Database" is defined as "a collection of information that is held by magnetic or optical means and that is intended for computer processing." The definition also excludes databases for personal use or databases that contain only contact information that does not make possible a violation of privacy, as long as the owner of the collection does not control any other databases.

Generally speaking, the Law applies to stored data concerning private individuals. It does not apply to information regarding corporations and business-oriented bodies.

The Law does not limit the type of data that can be collected. However, other laws might prohibit the collection of some forms of data.

The Law defines "information" as data on a person's personality, personal status, private family relations, state of health, economic position, vocational qualifications, opinions and beliefs. It defines "sensitive information" as:

1. Data on a person's personality, private family relations, state of health, economic condition, opinions and faith.

2. Information which the Minister of Justice – by order with approval by the Knesset Constitution, Law and Justice committee – designated as sensitive information.

The definitions of "information" and "sensitive information" are similar. However, data regarding personal status and professional qualifications are not considered sensitive information.

PRIVACY CASE STUDIES

In the "Bank Hapoalim" precedent (Civil Action Number 86/1989), the

then president of Israel's High Court, Meir Shamgar, ruled that "data" should be interpreted in a way that will fulfil the purpose of the Law, which is also to protect the economic status of a person's privacy. Thus, President Shamgar ruled that the Law applies not only to databases which are organised on a personal basis (meaning by names), but also to databases which are organised in other ways, if those databases can reveal the economic status of a person. In the "Bank Hapoalim" case, the database was organised by automobile licence numbers.

The "Ventura" case (Civil Action Number 439/1988) concerned a company that wished to register a blacklist of people whose cheques had been presented for payment but were not supported by sufficient funds. Judge Bach ruled that the natural interpretation of the words "personal matters" is "any information which relates to one's personal life, including his name, address, telephone number, and working place, as well as the identity of his friends, his relations with his wife and other members of his family."

Details that usually are not regarded as personal may, in combination, be regarded as information regarding personality or other personal matters. Therefore, information compiled from different databases that may hint at the creditworthiness of a particular individual may be considered as information about their personal and financial situation.

The use of information is limited to the use for which it was given by the individual, unless the individual gives explicit consent for a different use. Consent is also required in connection with the publication of the information. A person may give personal information to a certain body or to the public, but may object to a transfer of such data to others. Therefore, before using personal information, it is essential to check the scope of the consent.

Publishing data that was illegally collected or that was collected while invading an individual's privacy – for example, data taken from another database assembled for other purposes – is illegal and constitutes a violation of privacy. The Law provides a defence only if the published data is accurate and true, and only if a public interest justifies the violation.

Therefore it is crucial for those working with information to be cautious about the sources of the information. In addition, to ensure the required balance between the public interest and privacy, the individual should be informed that a database contains information about him, and he should be allowed to review the information and request any necessary correction before it is disseminated.

Section 8 of the Law sets out the duty to register databases and imposes limits on using the data. It provides that: "A person will not manage or hold a database, which must be registered by this section, unless such a database was registered or its registration is already in process."

Section 8(c) specifies when the owner of the database must register the database. Registration is required when:

1. The database includes data about more than 10,000 people.

2. The database includes sensitive information.

3. The database includes data about people that was not provided by those people, or on their behalf, with their consent.

4. The database belongs to a public body.

5. The database is intended to be used for direct mailing (this includes sending by fax, telephone and email).

Section 8(b) of the Law prohibits use of data that must be registered for purposes other than those for which the database was established.

Since section 8 prohibits use of the data for purpose other than the original purposes, those registering databases should describe broad and general purposes in their applications for registration.

Registration Application

Section 9 identifies the details required in an application for registration of a database. Section 10 describes the broad discretionary authority of the registrar and the procedure for appeals concerning the registration process. It also establishes an inspection unit to carry out inspections and seizures of anything connected with databases. The inspection unit acts under the authority of the registrar.

Right of Inspection

Individuals have a right to inspect and challenge information held about them in a database. These rights are contained in the Protection of Privacy Regulations (conditions for the inspection of information and appeal procedures against the refusal of an inspection request) – 1981 (the "Inspection Regulations").

The Law gives no right to inspect information that is not computerised. It also does not prohibit the transfer of non-computerised information between public bodies.

Every person is entitled to inspect any information about him kept in a database. However, this right of inspection does not exist in respect of databases of a security authority, meaning the Israeli police, the military police of the Israel Defence Forces, the Intelligence Branch of the general staff, and the General Security Service. The Law also contains several other exceptions to the right of inspection.

The Inspection Regulations establish a mechanism to appeal against the refusal by the owner of a database to allow an inspection.

Transmission of Information by Public Bodies

Section 23 defines public bodies as government departments and other state institutions, local authorities and any other body carrying out lawful public functions. Public bodies also include bodies designated by the Minister of Justice if the designation specifies the categories of information and items that the body is entitled to deliver and receive. Hospitals have been designated in this manner.

Section 23B of the Law provides that the transmission of information

by public bodies is permitted only when the information has been published under lawful authority or made available for public inspection under lawful authority, or if the person to whom the information relates consents. In addition, in the "Bank Hapoalim" case, President Shamgar ruled that "the permission to transmit information [in section 23B] is also the duty to transmit the information when there are no reasonable reasons not to do so."

Section 23C contains exceptions to the general rule prohibiting the delivery of information by public bodies without the consent of the individual. For example, the prohibition does not apply to a "security authority" as defined in Section 19 of the Law.

Other obligations of public bodies are set out in sections 23D and 23E of the Law.

Special duties for the management and holding of a database (Sections 17A, 17B)

The Law defines the holder of a database as the one who holds a database in his permanent possession and who is entitled to use it. A database manager is "the active manager of a body that owns or holds a database or a person authorised by the manager..."

Those holding a small number of databases for different owners must allow access only to those which were identified in a written agreement between the holder and the owner of the database. Those holding more than five databases must appoint a person to be in charge of the security of the information. Public bodies, banks, insurance companies and credit evaluation companies must also make such an appointment.

Special duties and regulations for direct mailing

The Law contains specific provisions on direct mailing. Direct mailing is defined as "an individual approach to persons, based on their belonging to a population group determined by one or more characteristics of persons whose names are included in a database."

The term "approach" includes approaches in writing, by facsimile, in print, and by mail, e-mail and other computerised types of information transfer.

Direct mailing services are defined as the direct mailing of lists, labels or data "by any means whatsoever."

Among the special obligations that apply to operators of direct mailing services are:

- The duty to register the database that is used for the service.

- The duty to keep a record of the source of any data used for the direct mailing service, as well as the date it was accepted and to whom the data was transferred.

- The duty to inform individuals that the mail they receive is direct mail, the registration number of the database that serves the direct mailing and the source of the data. The approach also should mention the right of the recipient to be deleted from the database.

- The entitlement of every person to demand that the owner of the database being used for direct mailing services delete any data relating to him, or that personal details are not disclosed to certain persons or categories of persons, either temporarily or permanently.

These duties place a heavy burden on direct mailing companies. Since the definition of a direct mailing approach includes telephone calls, telemarketing companies are forced to bear this burden as well.

Criminal punishments

Section 31A identifies the offences under the Law. Among the offences that may lead to imprisonment for up to one year:

- Managing, holding or using a database that acts in a way that contradicts the instructions of Section 8 of the Law.

- providing false details in a registration application.

- providing false details in a notice attached to a request for information under section 11, or not providing the required details.

To date, no person appears to have been sentenced to incarceration under this law.

There is no need to prove criminal intent or negligence to succeed with a prosecution for the offences listed in section 31A. Moreover, these offences are also considered as civil wrongs.

Transferring data out of Israel

The articles of the protection of privacy (the transfer of data outside of the country's borders) – 2000 (the "Articles") regulate the transfer of data from Israel. The Articles seek to ensure that data is not transferred to any country that provides less privacy protection than Israel.

Naomi Assia is an Israel-based lawyer and lecturer, specialising in intellectual property, computer software and data protection. She is the founder of the Naomi Assia Law Offices and also serves on a number of legal committees, including the Israeli Committee on Privacy.

She can be contacted at:
Tel: +972 3644 4808, e-mail: nassia@computer-law.co.il

This report is based on an extract from Assia's book, "Computer Law", published by N.D.I.R Computers Ltd