Israeli data protection law: constitutional, statutory and regulatory reform

Dr Omer Tene, a Lecturer and member of the Israeli Ministry of Justice Committee for reform of data protection law, compares the Israeli and European Data Protection Principles, analyses the reforms suggested by the Schofman report, and evaluates the compliance and enforcement improvements made by Israel's newly established data protection authority

Israeli data protection law is in flux. The right of privacy has been elevated to constitutional status and consequently has encouraged the Israeli Supreme Court to extend privacy and data protection beyond the scope of the Privacy Protection Act of 1981 ('PPA'). The PPA too is changing. Driven by technological developments and the will to harmonise Israeli law with European standards, a government committee has recently proposed a wholesale reform of the statute's data protection chapter. To increase compliance and enforcement levels, Israel has established a new data protection authority – the Israeli Law and Information Technologies Authority – to replace the former Database Registrar.

This article reviews the spate of recent changes to Israeli data protection law and comments on persisting discrepancies between Israeli and European data protection.

Constitutional reform

At its inception in 1948, Israel was a non-constitutional democracy and was based on the UK model. Over recent decades, Israel has systematically shaped its Constitution, much like the Canadian system, through the enactment of 'Basic Laws.' The right to privacy was elevated to constitutional status in Israel in 1992. Yet, only in the past few years have Israeli courts acknowledged the importance of privacy, and its position near the top of the normative pyramid.

The legal effects of privacy entering into the Israeli constitution have been profound, impacting, for example, the law of evidence, government search and seizures, freedom of speech and the press, and data protection.

Israeli constitutional law grants courts the power to strike down statutes infringing on basic constitutional rights. Moreover, the Israeli Supreme Court has held that constitutional principles apply to private sector transactions, and not solely to government action.

In the case of *Association of Human Rights v Ministry of Interior* [2004], the Israeli Supreme Court ruled that some public sector data sharing practices, as well as data transfers from the Ministry of Interior to private sector financial institutions, were unconstitutional. The Court held that although such data transfers had been authorised by statute, they were overly broad and had a disproportional effect on data subject privacy.

The Supreme Court ruled that data transfers must be restricted by regulations specifying the precise recipients, use of data, and data security measures. It provided that transfers to financial institutions must be expressly authorised by statute; anti-money laundering regulations do not suffice.

The ruling in the *Association of Human Rights* case signifies Israeli courts' willingness to extend the constitutional framework from "core" privacy issues to data protection law.

Data protection practitioners should thus be aware that even if certain transactions or practices satisfy the PPA, they remain subject to constitutional review under the 'Basic Law.' Section 8 of the 'Basic Law' provides that constitutional rights may be infringed only by statute, which is consistent with the values of the State of Israel, enacted for a proper purpose and restricts rights to an extent no greater than is necessary. An employer, for example, wishing to transfer employee personal data to a third party must comply not only with the provisions of the PPA but also with the constitutional principles of legality, proper purpose and proportionality.

Statutory reform

Dating from 1981, the PPA – and Chapter B thereof, which deals with data protection – is one of the first data protection statutes in the world. As such, it has become outdated and in need of reform.

In 2005, the Israeli Ministry of Justice set up an expert committee charged with reviewing and propos-

(Continued on page 8)

(Continued from page 7)
ing comprehensive reform of the data protection chapter of the PPA. The committee, headed by Deputy Attorney General Yehushua Schofman, consisted of government officials, academics, private sector lawyers, and representatives of non-governmental organisations.

The committee's mandate cited the deep technological transformation since the inception of the PPA, as well as the need to harmonize Israel's data protection regime with that of the European Union.

Redefining "data"

In January 2007, the committee handed its report (the 'Schofman Report') to the Ministry of Justice, which is currently drafting a comprehensive bill based on the recommendations. The Report of the Committee for Review of Data Protection Legislation (Jerusalem, 2007) is available at the Ministry of Justice site: www.justice.gov.il/mojeng (in Hebrew).

The Schofman Report reviews the basic definitions and scope of Israeli data protection law. It recommends changing the central definition of the data protection regime – that of "personal data," or as used in the PPA, "data."

The term "data" is currently defined in section 7 of the PPA as "details concerning an individual's personality, personal status, intimate relations, health condition, financial condition, professional experience, opinions and religious belief."

The definition is confusing, especially when compared to similar terms used throughout the PPA, such as "information concerning an individual's private matters," (sections 2(7), 2(8) and 2(9) of the PPA); "matters relating to an individual's intimate private life," (section 2(11) of the PPA); and, most conspicuously, the definition of "sensitive data" — "details concerning an individual's personality, intimate relations, health condition, financial condition, opinions and religious belief" (section 7 of the PPA). Thus currently, the sole difference between the definition of "data" and that of "sensitive data" is that the former includes "details concerning an individual's… personal status" and "professional experience," which are not categories in the latter definition. Moreover, the current definition of "data" excludes certain categories of information which apparently belong within the data protection framework, such as customer lists and purchase history.

The Schofman Report recommends overcoming these difficulties by shifting to a European-style definition of personal data: "any information relating to an identified individual or one identifiable by reasonable means" (section 3(1) of the Schofman Report). The new term used would be "personal data," much like in European data protection legislation, as opposed to the current "data." In addition, the definition of "sensitive data" would be entirely deleted from the PPA.

Computerised databases

An additional adjustment to the scope of the Israeli data protection statute concerns manual files and records. The PPA currently applies strictly to computerised databases. The Schofman Report proposes expansion of the law to non-computerised databases. It cites concerns over circumvention of the law (for example, by printing out records and maintaining them in paper form), as well as the fact that large, historical non-computerised databases (for example, those held by the social security administration or by health insurers), remain data protection liabilities.

This proposal will broaden the scope of the law, which could in itself create difficulties. Some critics believe this expansion is unnecessary, since non-computerised databases are becoming obsolete; and the application of the law to manual files and records raises severe definitional problems; for example, when does a collection of documents become "structured" enough to be considered a "database," see *Durant v Financial Services Authority* [2003] EWCA Civ 1746.

Database registration

The main thrust of the Schofman Report is twofold: to relax database registration requirements, and to increase compliance and tighten enforcement through private and regulatory means.

Current database registration requirements are broad. Section 8(c) of the PPA provides that a database must be registered with the Database Registrar if it:

(a) includes data concerning more than 10,000 data subjects;

(b) includes sensitive data;

(c) includes data which have not been provided by individual data subjects, on their behalf or with their consent;

(d) is a public sector database; or

(e) is used for direct marketing services.

Critics of the current situation argue that merely 2% of existing databases falling under one of the section 8(c) categories are in fact registered. Hence, the vast majority of data controllers do not comply with the law. Moreover, the Database Registrar placed too much weight on overseeing registration requirements but under-invested in compliance and enforcement actions.

Finally, registration might be misleading, creating in data subjects the false impression that registered databases comply with the law, whereas registration constitutes only one of several statutory requirements and is certainly no "seal of approval" by the Database Registrar.

The Schofman Report recommends restricting registration obligations to data brokers and databases including specific categories of data (that is "sensitive data" under the statute's current parlance). The Schofman Report would eliminate the defined term "sensitive data" (which appears nowhere else in the PPA besides sections dealing with registration requirements), and replace it with a list of specific categories of data that warrant database registration, namely medical data, genetic data, biometric data, matters relating to an individual's intimate private life, criminal records, and information concerning an individual's political or religious beliefs.

Enforcing data protection

Concurrent with its recommendations for relaxing registration requirements, the Schofman Report introduces statutory measures to increase data protection enforcement.

First, the Schofman Report would add the PPA to an existing list of statutes under which plaintiffs may file class action law suits. Second, it advocates a security breach notification mechanism modelled on California's 2003 statute (California Security Breach Information Act (West Supp. 2006)) which has been adopted in more than 30 US states. Third, while not part of the Schofman Report, a recent amendment to the PPA provides certain victims of privacy violations with compensation without proof of damage in an amount of 50,000 NIS ($10,000).

"Counter to European data protection law, which provides additional bases for processing besides consent, Israeli law requires consent, explicit or implicit, for any processing activity."

The main measure intended to increase data protection enforcement is the establishment of a new data protection authority, the Israeli Law and Information Technologies Authority ('ILITA'). Before beginning to describe the new ILITA, it is worth discussing a couple of issues that the Schofman Report does *not* address.

PPA conditions of lawful processing

The Schofman Report does not add any further conditions (or criteria) for fair and lawful data processing to the single existing PPA condition, data subject consent. Counter to European data protection law, which provides additional bases for processing besides consent, Israeli law requires consent, explicit or implicit, for any processing activity. Strictly speaking, the PPA requires *notification* of the data subject, of the purposes of processing and any recipients of data (section 11 together with section 8(b) of the PPA). Yet notification may be perceived as implicit consent, and lack of consent constitutes an element of any invasion of privacy cause of action (section 1 of the PPA). Under a recent amendment to the PPA, consent must be "informed."

Any business transactions and intra- and inter- entity data transfers, that do not have clear initial consent by data subjects, are therefore difficult to execute under the current regime. The lack of additional conditions for processing may compel controllers to solicit consent from large and diffuse groups of customers, suppliers or employees – often with high administrative costs.

An additional problem is that the Schofman Report does not add Data Protection Principles to those already provided by the PPA. A minority of Schofman Committee members supported raising the statutory bar in terms of Data Protection Principles, alongside lowering the statutory bar for database registration.

The PPA does not include principles equivalent to the First, Third and Fourth Principles under the UK Data Protection Act, that is, personal data being processed fairly and lawfully; adequate, relevant and not excessive; and kept for no longer than is necessary. While some may argue that these missing principles may be read into Section 2(9) of the PPA, the omission of these principles does not bode well for Israel's request for an adequacy finding under Article 25 of the EU Data Protection Directive.

Finally, a separate legislative reform would address direct marketing and unsolicited communications. Section 17F of the PPA currently imposes an opt-out regime for direct marketing, allowing companies to target data subjects as long as they do not object to being approached. A pending government sponsored bill (Draft Telecom Act: Telephone and Broadcast, 2005) would harmonise Israeli law with Article 13 of the Communications Privacy Directive (Directive 2002/58/EC).

The sponsored bill provides an opt-in regime for unsolicited communications by automatic calling machines, fax, email and SMS, including a "soft" opt-in for existing customers. Direct marketing methods involving human intervention or regular mail would continue to be governed by Section 17F of the PPA.

ILITA and regulatory reform

Regulatory enforcement of Israeli data protection law has traditionally been lenient. This leniency was mainly due to the lack of independence given to the main regulatory agency – the Database Registrar – a unit of the Ministry of Justice. In addition, the Database Registrar has been under funded and under staffed, employing less than 10 professionals, only a couple of whom were lawyers. The Database Registrar focused almost exclusively on verifying compliance with registration requirements – for the most part unsuccessfully. It rarely engaged in litigation and was not authorised to administer fines. This ineffective enforcement capability is demonstrated by the fact that only one case initiated by the Database Registrar has ever reached the Supreme Court (*State of Israel v Ventura*, 1994)

As part of the effort to increase data protection compliance and law enforcement, Israel established a new data protection authority in 2006, the ILITA. The ILITA has been charged with enforcing three statutes, the PPA, the Digital Signature Act 2001 and the Credit Reporting Act 2002. The ILITA is better funded and staffed than the Database Registrar, and most importantly, it intends to focus on compliance and enforcement. Moreover, under recent regulations, the ILITA has been authorised to administer fines (Administrative Offences

(Continued on page 10)

(Continued from page 9)
Regulations: Administrative Fines – Privacy Protection, 2004).

The recently appointed Head of the ILITA has already initiated investigations into high profile cases, such as the divestiture by Israeli banks of provident funds. The divestiture, which was mandated by the government in its effort to reduce concentration in the financial services industry, raised questions concerning use of customers' personal data by banks (the funds' sellers) and insurance companies (the buyers).

The Schofman Report proposes reinforcing the status of the ILITA by increasing its independence. While remaining a unit of the Ministry of Justice, the ILITA would be granted standing to join data protection litigation independently of the Attorney General. The Schofman Report explains that ILITA independence is vital due to the state's status as a major data controller and the broad range of public interests besides privacy which must be advanced by the Attorney General.

The Schofman Report further suggests empowering the ILITA to issue binding legal guidance, as well as data security orders addressed to specific data controllers. Finally, the ILITA would play a key role in the security breach notification system. It would serve as a central agent for breach notices, determine requisite notification methods, approve delays for law enforcement purposes, and maintain a record of security breaches.

International reform

Israel has recently applied for an adequacy ruling under Article 25 of the EU Data Protection Directive. Removing a potential trade barrier with the EU, its largest trading partner, is critical for Israel. Moreover, the adequacy of Israeli data protection law is vital for national security and law enforcement agencies, in the struggle against terrorism, money laundering, human trafficking and other serious crimes. While the EU Commission has yet to issue a formal assessment of Israeli data protection law, certain matters may be pointed out.

First, Israeli data protection law is in most respects more "adequate" than that of the United States. In comparison to the US, Israel has a comprehensive privacy and data protection regime as well as a dedicated enforcement agency. However, while black letter law appears adequate, compliance and enforcement levels tell a different story. As discussed above, enforcement, both regulatory and private, has been deficient for many years.

Second, even after all these anticipated reforms, the Israeli data protection authority will fall short of the "complete independence" standard set in Article 28 of the EU Data Protection Directive. The ILITA would remain a unit of the Ministry of Justice, subject administratively to the Minister of Justice and professionally to the Attorney General.

Finally, certain elements of Israeli data protection law will remain inconsistent with equivalent European provisions. For example, Israeli law does not include the "adequate, relevant and not excessive" or "kept for no longer than is necessary" principles; nor does it specify conditions for fair and lawful processing beyond data subject consent.

Conclusion

The elevation of the right of privacy to constitutional status reverberates through Israeli data protection law and regulations. The Schofman Report attempts to make data protection law more effective by clarifying the scope of the statute, changing the regulatory focus from database registration to compliance with substantive standards, and introducing mechanisms for private and regulatory enforcement. Under ILITA, the new data protection authority, public awareness of data protection and the legal risk associated with non-compliance are set to increase.

Dr Omer Tene
College of Management,
School of Law
tene.omer@gmail.com