BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

Reforming the Law from the Ground Up: Recent Developments in Israel's Privacy Regulation

BY OMER TENE

For many years, Israel's privacy and data protection law, which dates back to 1981, did not figure prominently in compliance programs of domestic and foreign companies operating in Israel, due to scarce enforcement activity and low public awareness. The establishment of the Israeli Law, Information and Technology Authority (ILITA) in 2006 and its active enforcement stance have changed this. In a period of just 2-3 years, amid a flurry of regulatory and individual enforcement activity, data protection has become a significant factor for compliance officers and chief information officers in Israel, particularly in the data-rich financial services, telecom and health sectors. With the EU data protection regulators' ''adequacy'' opinion and the decision of global regulators to be hosted in Jerusalem for their 32nd annual conference, Israel catapulted to the center of global attention.

Dr. Omer Tene is a legal consultant and Associate Professor, College of Management School of Law, Rishon Le Zion, Israel. He may be contacted at omer.tene@bezeqint.net.

The Adequacy Opinion. On Dec. 1, 2009, the EU Article 29 Working Party published an opinion finding that Israeli data protection law largely provides an ''adequate level of data protection'' under EU Data Protection Directive 95/46/EC (the ''Directive'').[1] The opinion is restricted to automated data processing, given that Israel's data protection statute, Chapter B of the Privacy

[1] Article 29 Data Protection Working Party, Opinion 6/2009 on the level of protection of personal data in Israel, 02316/09/EN, WP 165, 1 December 2009, available at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp165_en.pdf.

 ISSN 1538-3423

Protection Act, 1981 (''PPA''), does not apply to manual databases. In their opinion, the 27 European data protection regulators acknowledge that the PPA complies with the fundamental principles of the Directive, including purpose limitation, proportionality, transparency, security, right of access and rectification, and restrictions on onward transfers. In addition, the Article 29 Working Party certifies that Israel's privacy regulator, ILITA, ''possesses the necessary independence and the adequate enforcement competencies, in similar terms to those provided by Article 28 of the Directive.'' This is a noteworthy development, given that ILITA is part of the Israeli Ministry of Justice. Thus, the Article 29 Working Party accepted Israel's argument that while formally part of the government apparatus, ILITA is independent when assessed under substantive criteria. This decision may mark an important new path for additional countries whose constitutional and administrative structure is different than yet compatible to that of EU Member States.

Another sign of Israel's integration into the global privacy community is its selection as host of the 32nd annual conference of data protection and privacy commissioners as well as the event marking the 30th anniversary of the Organization for Economic Cooperation and Development Privacy Guidelines. The events, scheduled for Oct. 26-29, will bring hundreds of participants and more than 120 speakers to Jerusalem, including leaders from the regulatory, business, government, academia, and nongovernmental organization communities.

Legislation and Regulation

The Israeli Ministry of Justice has been engaged for several years in an effort to reform the data protection chapter of the PPA, in an attempt to adapt it to the technological sea change of the past three decades. The reform was due to be based on a February 2007 report by a public committee headed by former Deputy Attorney General Joshua Schoffman (the ''Schoffman Report''),[2] which suggested a shift in emphasis from the law's bureaucratic provisions (namely, database registration) to enforcement of substantive principles, such as data security and collection and use limitation. The Schoffman Report recommended significantly curtailing database registration requirements, making them the exception rather than the rule. In order to maintain the benefits of registration, including requiring organizations to map their data flows and providing regulators with an enforcement tool, registration would be replaced with a duty to conduct internal audits (or privacy impact assessments), and to implement ''proper database management'' procedures. While these legislative efforts have largely stalled, change continues to be driven by ILITA, other regulatory agencies, individuals and courts – effectively reforming the system from the ground up.

Legislative reform. So far, the only piece of the legislative reform package to reach Israel's parliament concerns the authority and powers of ILITA itself (the ''Enforcement Bill'').[3] Under the Enforcement Bill, ILITA would be authorized to impose civil sanctions in an amount of up to $1 million. In addition, ILITA would enjoy far reaching powers of interrogation, search and seizure, including, in limited circumstances, warrantless search of computer data.

In January, ILITA issued for public comment draft data security regulations, which apply to organizations processing data in both the public and private sector.

Data Security Regulations. On Jan. 10, ILITA issued for public comment draft data security regulations, which apply to organizations processing data in both the public and private sector.[4] The new regulations would require organizations to appoint an information security officer; set forth internal data security procedures; conduct periodic risk assessments and audits; pre-scan employees for security vulnerabilities; manage access authorizations; create audit trails; document potential security breaches; implement specific measures to protect information and communication systems and the storage or transfer of data on portable devices; contractually restrict outsourcing vendors; and ensure effective back up and disaster recovery. The regulations introduce not only detailed data security procedures but also substantive provisions which arguably exceed the scope of the PPA, including limits on data retention and a requirement that data collected are relevant and not excessive. The regulations are modular, dividing databases into risk categories based on both data sensitivity and the number of data subjects, and applying different rules to ''high'', ''medium'' and ''low'' risk databases.

Guidance on data subject authentication. In Feb. 11, ILITA issued a guidance note on the authentication of data subject identity for purposes of remote access to personal data. The premise for the guidance is that information traditionally used by organizations to authenticate customer identity, such as an individual's full address, date of birth or mother's maiden name, can no longer be used safely given the leakage of data from Israel's population register to illicit files and databases accessible on the Internet. ILITA warns that exclusive reliance for authentication purposes on information contained in the population register will be considered a violation of the PPA's data security and confidentiality provisions. ILITA requires that before providing a customer with access to his or her personal data or permitting password recovery, organizations must implement data security measures commensurate with the risk and sensitivity of the data. Such measures include

[2] Ministry of Justice Committee for the Examination of Legislation Relating to Databases, Final Report, 21 January 2007, available at http://www.justice.gov.il/NR/rdonlyres/B11D19EE-7FC0-42ED-B2F5-2B4FDEE66BD4/18343/SchoffmanReport1.pdf.

[3] Privacy Protection Bill (Amendment) (Enforcement Powers), 2010.

[4] *See* Draft for the Protection of Privacy Regulations (Information Security in Databases), 5770-2010, available at http://www.justice.gov.il/NR/rdonlyres/450A9F18-F22A-4D47-A408-47221D88BE24/18541/ProtectionofPrivacyRegulationsDraft25110.pdf.

  PVLR ISSN 1538-3423

verification of at least one item of information known exclusively to the data subject and not contained in the population register (*e.g.*, name of first pet or favorite rock star). The more sensitive the data, the more items of information that need to be verified. Alternatively, an organization may rely on ''something the user has'' (*e.g.*, a smart card or mobile phone) or ''something the user is'' (*e.g.*, a biometric identifier) in addition to ''something the user knows''. The guidance, which became effective on Aug. 1, created a stir among legal counsel and CIOs of large Israeli companies, who had to contemplate contacting millions of customers to roll-out new identity authentication schemes.

Supervisor of banks instruction concerning social networking sites. Not only ILITA but also additional market regulators have recognized the gravity of the operational and legal risks wrought by personal data. On July 28, 2010, the Israeli Supervisor of Banks issued a letter to chief executive officers of all local banks expressing concern over the banks' and their employees' use of social networking services, including both proprietary Web 2.0 tools and networking sites such as Facebook, Twitter and LinkedIn. The Supervisor of Banks identified the following operational and legal risks involved in social networking: identity theft (*e.g.*, using customer data to retrieve his or her password for online banking); the publication of false or misleading data by an employee or customer; data security breaches; and insufficient audit and control of service providers. The Supervisor of Banks required that certain measures be implemented to minimize such risks, including conducting a risk assessment by an outside expert; devising and verifying compliance with a social networking policy and detailed guidelines for customers and employees; and closely following uses, trends and risks inherent to the system. Collaboration among different market regulators, including banks, securities, consumer protection and antitrust authorities, is set to significantly reinforce consumer protection while posing an increased challenge for corporate compliance officers.

Financial sector regulation. A conspicuous example of privacy and data security instructions issued by regulatory agencies other than ILITA is the Supervisor of Banks' Regulation No. 357 on Information Technology Management (''Regulation 357''), as well as equivalent instructions issued by the Commissioner of Capital Markets, Insurance and Savings.[5] Regulation 357, which also applies to foreign banks operating in Israel, requires a series of measures to be implemented by banks with respect to information technology systems, including maintaining access logs and an audit trail; creating, publishing and implementing a data retention policy; conducting risk assessments, periodic audits and data security surveys; appointing a data security manager; ensuring authentication of customer identities; and integrating specific contractual provisions into outsourcing agreements. Electronic banking services are subject to more stringent measures under Chapter G of Regulation 357. Section 30(b) of Regulation 357 requires a report of any security breaches to the Supervisor of Banks. It thus constitutes Israel's first security breach notification regulation.

A financial sector regulation requires a report of any security breaches to the Supervisor of Banks. It thus constitutes Israel's first security breach notification regulation.

Regulatory Enforcement

Since its establishment in 2006, ILITA has stepped up enforcement efforts, in stark contrast to the traditionally lax enforcement stance of the former Database Registrar. Such efforts include carrying out spot checks on private and public sector controllers; issuing orders to Government departments to cease processing; and investigating security breaches at various organizations. Even before the passage of the Enforcement Bill, ILITA's investigators were authorized in July 2009 by the Chief of Police to conduct investigations under Israel's Criminal Procedure Ordinance (Testimony). In addition, Israel's parliament recently approved an increase in the maximum fines ILITA is authorized to levy.

Consequently, in the past few months, ILITA exercised its authority to levy fines in an amount of NIS 258,000 ($70,000) in a case concerning illegal trading of personal data; and NIS 176,000 ($50,000) in a case concerning illicit use of an illegal copy of the population register. In addition, ILITA imposed sanctions on public sector organizations, including the powerful Ministry of Defense in a case involving insufficient data security measures in an outsourcing transaction; and the Municipality of Ramat Gan in a case of illegal use of high school students' data for marketing purposes, in violation of the purpose limitation principle.

In perhaps its most significant enforcement action, ILITA intervened in a series of major transactions among banks and insurance companies, to limit the use of personal data held by subsidiary pension funds. In 2005, Israeli banks were mandated by bank and antitrust regulators to divest their holdings in pension funds in an effort to reduce concentration in the financial services sector. Consequently, the banks sold their holdings in the pension funds to insurance companies and other investment companies. The ensuing series of transactions, of significant scale and scope relative to the size of the Israeli market, raised a host of data protection issues. ILITA restricted the permitted uses of pension fund data; mandated that databases register under fund managers' names; and ordered insurance companies to cease sending marketing and promotional materials to pension fund customers.[6]

[5] *See, e.g.,* Instructions of the Commissioner of Capital Markets, Insurance and Savings, Circular 2006-9-6, Instruction on the Management of Data Security Risks by Institutional Investors (October 16, 2006); Instructions of the Commissioner of Capital Markets, Insurance and Savings, Circular 2009-166, Draft Instruction on the Management of Information Technology Systems by Institutional Investors (January 25, 2010).

[6] *See* Yoram Hacohen & Omer Tene, Transferal of Pension Fund Databases, 5(11) Data Protection Law & Policy 14 (Dec. 2008).

Individual Enforcement

Israel's privacy law combines regulatory enforcement, which is common in European jurisdictions, with individual enforcement mechanisms more characteristic of the United States. Individual enforcement tools include statutory damages in an amount of up to NIS 50,000 ($13,000), introduced in 2007 as an amendment to the PPA; class action lawsuits; and appeals to standard contract tribunals to modify or annul ''unfair'' terms in standard form contracts pursuant to the Standard Form Contracts Act, 1982.[7] The recent increase in individual enforcement reflects rising public awareness to privacy and data protection. Successful plaintiffs, in turn, are likely to attract media attention, increasing awareness even more and boosting regulatory enforcement by encouraging additional complaints.

Class actions. In the case of *Sudri v. Pelephone Communications Ltd.*,[8] plaintiffs sought damages from Pelephone, a mobile operator that had admitted to retaining users' text messages beyond the period necessary for their transmission. Intimidated by the prospect of a damaging class action, Pelephone announced that it would change its data retention practices in the case's first court hearing. Additional cases were brought under Israel's new anti-spam statute, Section 30A of the Telecommunications Act (Telephone and Broadcast), 1982, including requests to certify class actions in amounts exceeding $10 million. Section 30A is modeled on the European Electronic Communications Privacy Directive (2002/58/EC). It applies to businesses sending unsolicited commercial messages by electronic means, including automated calling systems, fax, e-mail, and text messages. It imposes stiff civil and criminal penalties, including directors' and officers' liability, and authorizes plaintiffs to file class action law suits.

[7] *See* App. (Jer.) 195/97 *Attorney General v. Bank Leumi* (10 June 2004), striking down data sharing provisions in Bank Leumi's account opening contract as unfair standard contract terms; Std. Contracts 8002/02 *Supervisor of Banks v. First International Bank for Mortgages* (5 May 2009), similar result for data transfer provisions of loan and mortgage agreement of First International Bank for Mortgages.

[8] Class Actions 21185-07-09 *Sudri v. Pelephone Communications Ltd.* (pending in Central District Court).

Another category of lawsuits that have recently become common is employees suing their employers for privacy infringements, particularly in the context of monitoring e-mail and Internet use.

Employee monitoring. Another category of lawsuits that have recently become common is employees suing their employers for privacy infringements, particularly in the context of monitoring e-mail and Internet use. In a case currently pending before the National Labor Court concerning employer e-mail monitoring, the Attorney General joined as *amicus* and asserted that any infringement of employee privacy must be assessed under the constitutional proportionality principle, regardless of whether the employer is in the public or private sector.[9] In a case recently decided in the Central District Court, the court applied the ''reasonable expectation of privacy'' test established by the U.S. Supreme Court[10] to hold that the monitoring of an employee's e-mail constitutes a breach of his right to privacy under the PPA, and may even constitute an illegal wiretap.[11] Consequently, it is important for employers operating in Israel to establish clear policies for use of communication systems and employee monitoring.

Conclusion

The lengthy period of time required to effect legislative change has not hampered the development of a vibrant regulatory landscape in Israel, based on enforcement actions of both ILITA and private litigants. Multinational companies operating in Israel should take account of recent regulatory actions and case law to minimize risk of corporate or directors and officers' liability.

[9] Lab. App. 90/08 *Issakof v. Panaya* (pending in the National Labor Court).

[10] *Katz v. United States*, 389 U.S. 347 (1967).

[11] App. Disc. Munic. Ct. (Center) 13028-04-09 *Benjamin Eliyahu v. Municipality of Tiberius* (2010).

  PVLR ISSN 1538-3423