The Privacy, Data Protection and Cybersecurity Law Review

Second Edition

Editor
Alan Charles Raul

Law Business Research

The Privacy, Data Protection and Cybersecurity Law Review

The Privacy, Data Protection and Cybersecurity Law Review
Reproduced with permission from Law Business Research Ltd.

This article was first published in The Privacy, Data Protection and Cybersecurity Law Review - Edition 2
(published in November 2015 – editor Alan Charles Raul)

For further information please email
Nick.Barette@lbresearch.com

The Privacy, Data Protection and Cybersecurity Law Review

Second Edition

Editor

Alan Charles Raul

Law Business Research Ltd

PUBLISHER
Gideon Roberton

SENIOR BUSINESS DEVELOPMENT MANAGER
Nick Barette

SENIOR ACCOUNT MANAGERS
Katherine Jablonowska, Thomas Lee, Felicity Bown, Joel Woods

ACCOUNT MANAGER
Jessica Parsons

PUBLISHING MANAGER
Lucy Brewer

MARKETING ASSISTANT
Rebecca Mogridge

EDITORIAL ASSISTANT
Sophie Arkell

HEAD OF PRODUCTION
Adam Myers

PRODUCTION EDITOR
Robbie Kelly

SUBEDITOR
Gina Mete

MANAGING DIRECTOR
Richard Davey

Published in the United Kingdom
by Law Business Research Ltd, London
87 Lancaster Road, London, W11 1QQ, UK

www.TheLawReviews.co.uk

ISBN 978-1-909830-75-2

Printed in Great Britain by
Encompass Print Solutions, Derbyshire
Tel: 0844 2480 112

THE LAW REVIEWS

THE MERGERS AND ACQUISITIONS REVIEW

THE RESTRUCTURING REVIEW

THE PRIVATE COMPETITION ENFORCEMENT REVIEW

THE DISPUTE RESOLUTION REVIEW

THE EMPLOYMENT LAW REVIEW

THE PUBLIC COMPETITION ENFORCEMENT REVIEW

THE BANKING REGULATION REVIEW

THE INTERNATIONAL ARBITRATION REVIEW

THE MERGER CONTROL REVIEW

THE TECHNOLOGY, MEDIA AND
TELECOMMUNICATIONS REVIEW

THE INWARD INVESTMENT AND
INTERNATIONAL TAXATION REVIEW

THE CORPORATE GOVERNANCE REVIEW

THE CORPORATE IMMIGRATION REVIEW

THE INTERNATIONAL INVESTIGATIONS REVIEW

THE PROJECTS AND CONSTRUCTION REVIEW

THE INTERNATIONAL CAPITAL MARKETS REVIEW

THE REAL ESTATE LAW REVIEW

THE PRIVATE EQUITY REVIEW

THE ENERGY REGULATION AND MARKETS REVIEW

THE INTELLECTUAL PROPERTY REVIEW

THE ASSET MANAGEMENT REVIEW

THE PRIVATE WEALTH AND PRIVATE CLIENT REVIEW

THE MINING LAW REVIEW

THE EXECUTIVE REMUNERATION REVIEW

THE ANTI-BRIBERY AND ANTI-CORRUPTION REVIEW

THE CARTELS AND LENIENCY REVIEW

THE TAX DISPUTES AND LITIGATION REVIEW

THE LIFE SCIENCES LAW REVIEW

THE INSURANCE AND REINSURANCE LAW REVIEW

THE GOVERNMENT PROCUREMENT REVIEW

THE DOMINANCE AND MONOPOLIES REVIEW

THE AVIATION LAW REVIEW

THE FOREIGN INVESTMENT REGULATION REVIEW

THE ASSET TRACING AND RECOVERY REVIEW

THE INTERNATIONAL INSOLVENCY REVIEW

THE OIL AND GAS LAW REVIEW

THE FRANCHISE LAW REVIEW

THE PRODUCT REGULATION AND LIABILITY REVIEW

THE SHIPPING LAW REVIEW

THE ACQUISITION AND LEVERAGED FINANCE REVIEW

THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW

THE PUBLIC-PRIVATE PARTNERSHIP LAW REVIEW

THE TRANSPORT FINANCE LAW REVIEW

THE SECURITIES LITIGATION REVIEW

THE LENDING AND SECURED FINANCE REVIEW

THE INTERNATIONAL TRADE LAW REVIEW

www.TheLawReviews.co.uk

ACKNOWLEDGEMENTS

The publisher acknowledges and thanks the following law firms for their learned assistance throughout the preparation of this book:

ADVOKATFIRMAET SIMONSEN VOGT WIIG AS

ALLENS

ASTREA

BOGSCH & PARTNERS LAW FIRM

CMS CAMERON MCKENNA GRESZTA I SAWICKI SP.K.

DUNAUD CLARENC COMBLES & ASSOCIÉS

ELIG, ATTORNEYS-AT-LAW

JUN HE LAW OFFICES

LEE & KO

MATHESON

MATTOS FILHO, VEIGA FILHO, MARREY JR E QUIROGA ADVOGADOS

NNOVATION LLP

PEARL COHEN ZEDEK LATZER BARATZ

SANTAMARINA Y STETA, SC

SIDLEY AUSTIN LLP

SUBRAMANIAM & ASSOCIATES

URÍA MENÉNDEZ ABOGADOS, SLP

VIEIRA DE ALMEIDA & ASSOCIADOS, RL

WALDER WYSS LTD

WINHELLER RECHTSANWALTSGESELLSCHAFT MBH

CONTENTS

Chapter 15

ISRAEL

Haim Ravia and Dotan Hammer[1]

I OVERVIEW

The right to privacy is fundamental under Israeli law. Article 7 of the Basic Law: Human Dignity and Liberty establishes a constitutional right to privacy.[2] In addition, Israeli law includes an omnibus privacy and data protection statute, the Protection of Privacy Law, 5741-1981 (PPL).[3] Other statutes govern particular data protection issues, such as the Credit Data Services Law, 5762-2002 (CDSL), that governs the collection and dissemination of data regarding the creditworthiness of individuals and sole proprietors and the Patient Rights Law, 5756-1996,[4] which governs medical treatment of patients and the protection of patients' medical and health information.

Various regulations promulgated under the PPL set rules and procedures for retaining and safeguarding personal data, transferring it between public entities, granting data subjects the right to access, amend and delete personal information, and cross-border transfer of personal data.

The Registrar of Databases (the Registrar), is the regulatory authority under the PPL. The Registrar operates within the Israeli Law, Information and Technology Authority (ILITA) at the Ministry of Justice. Alongside its regulatory enforcement powers, the Registrar occasionally releases guidelines on data protection and privacy.

---

1 Haim Ravia is a senior partner and Dotan Hammer is a senior associate at Pearl Cohen Zedek Latzer Baratz.

2 For an English translation of the Basic Law: Human Dignity and Liberty, see: www.knesset.gov.il/laws/special/eng/basic3_eng.htm.

3 An unofficial translation of the Protection of Privacy Law is available at: www.wipo.int/edocs/lexdocs/laws/en/il/il084en.pdf.

4 An unofficial translation of the Patient Rights Law is available at: http://waml.haifa.ac.il/index/reference/legislation/israel/israel1.htm.

These guidelines are not legally binding per se, but represent the Registrar's position and may therefore serve as guiding principles for its exercise of enforcement powers. In recent years, the Registrar has issued guidelines on topics such as commissioning outsourcing services for processing personal information, the applicability of the PPL to employee placement services and screening processes, and the use of security and surveillance cameras.

II THE YEAR IN REVIEW

This year the Bank of Israel (Israel's central bank) issued notable guidelines on the use of cloud computing services by banking corporations and credit card companies, and on cyberdefence management. Contrarily, ILITA's impact on the data protection landscape has been less evident.

Over the past year, the Israeli government has been vigorously promoting cyberdefence issues. It began establishing a national authority for cyberdefence, within the Israeli Prime Minister's Office. This step followed the establishment in 2011 of the National Cyber Bureau in the Prime Minister's Office, whose role is to devise an Israeli national defence doctrine on cyberspace.

This year, the Israeli government published a draft bill aimed at extensively amending the CDSL. Presently, pursuant to the CDSL, various entities that possess information on the creditworthiness of individuals and sole proprietors are required to make that information available to licensed Credit Reporting Agencies, who are in turn authorised to disseminate the information subject to certain conditions and limitations.

The new draft bill proposes collection of data intended to be used in assessing the risk that credit seekers will default on their loans. Such data will include, among other things, the so-called 'positive information' about payment obligations that individuals and organisations have undertaken and whether or not they have met the payment schedule. Those who wish may elect to opt out of having such information collected and processed about them. The proposed amendment aims to reduce the cost of credit by boosting competition in the credit market, for the benefit of households and small businesses. This draft bill still needs to be proposed as a bill at the Knesset (the Israeli parliament) and then passed into law.

The past year has witnessed an unprecedented leak of credit cardholders' information. Former employees of Leumi Card, an Israeli issuer of the internationally renowned Visa credit card, had stolen data on one million cardholders and then tried to extort large sums of money from Leumi Card. They were apprehended and indicted in 2015, and their trial continues. The stolen data was not disseminated.

III REGULATORY FRAMEWORK

i Privacy and data protection legislation and standards

Chapter 1 of the PPL lays down the framework on invasion of privacy under Israeli law. It specifies an exhaustive set of more than a dozen eventualities, each constituting an actionable civil tort of invasion of privacy if committed without the informed consent of

the individual who is the subject of the privacy-invading conduct.[5] For instance, using, disclosing or transferring information regarding the 'private affairs' of an individual, for purposes other than for which it was given, constitutes invasion of privacy in the absence of the informed consent of the individual. The term 'private affairs' in this respect has been held by the Israeli Supreme Court to mean every piece of information related to a person's private life, including his or her name, address, contact information, and details of workplace, friends and family.[6] Most eventualities enumerated in Chapter 1 of the PPL also give rise to a criminal offence punishable by up to five years' imprisonment, if committed maliciously.[7] Invading the privacy of an individual by way of unlawfully penetrating a computer to access computerised data can also give rise to criminal liability under the Computers Law, 5755-1995.

The PPL and Israeli law in general, only protect the privacy of individuals.[8] Corporations and other legal entities are not afforded privacy under Israeli law.

Chapter 2 of the PPL addresses personal data processing. It revolves around the notion of a 'database', defined in the statute as a collection of 'information' elements held in a magnetic or optical medium and intended for computerised processing (with some exceptions).[9] The term 'information' is defined as data regarding an individual's personality, familial status, intimate affairs, health or medical condition, financial status, professional qualifications, opinion or beliefs.[10]

The PPL and the regulations promulgated thereunder prescribe various duties and obligations with respect to databases. These include a statutory duty to register most kinds of database with the Registrar,[11] a duty to allow data subjects to exercise their right to review, correct or delete erroneous or outdated data about them stored in a database,[12] a duty to provide data subjects notice with certain details when seeking their information for the purpose of using it in a database[13] and a duty to implement information security measures.[14] Chapter 2 of the PPL also governs the use of databases for 'direct mailing' purposes, a term defined as contacting a person (such as by written communications, telephone, fax or computerised means) under some characteristic-based profiling or segmentation.[15]

---

5 Sections 1–3 of the PPL.

6 Civil Appeal 439/88 *Registrar of Databases v. Ventura*, PD 48(3) 808 (1994).

7 Section 5 of the PPL.

8 Section 3 of the PPL (definition of 'person').

9 Section 7 of the PPL (definition of 'database').

10 Section 7 of the PPL (definition of 'information').

11 Sections 8–10 of the PPL.

12 Sections 13–15 of the PPL and the Protection of Privacy Regulations (Conditions for Viewing Information and Procedures for Appealing Declined Requests to View), 5741-1981.

13 Section 11 of the PPL.

14 Section 17 of the PPL and the Protection of Privacy Regulations (Conditions for Possessing and Protecting Data and Procedures for Transferring Data between Public Bodies), 5746-1986.

15 Sections 17C–17I of the PPL.

The PPL distinguishes between a database owner, who has the primary title and interest in the database, and a database holder, who is a person or entity that has permanent possession of the database (or a copy of it) and is permitted to use it.[16] The term 'database owner' is not defined in the PPL. However, the Registrar maintains the position that the owner is the entity for whose needs the personal data is collected for processing from data subjects.

There are some conceptual similarities between a database owner under Israeli law and a data controller under EU data protection law, and likewise between a database holder under Israeli law and a data processor under EU data protection law. However, there are key differences in terms of the triggers, rights and obligations that database owners and holders have under Israeli law, compared with the triggers, rights and obligations that controllers and processors have under EU data protection law.

ii General obligations for data handlers

The PPL provides that any request made to data subjects that seeks information (as defined in the statute) for the purpose of using it in a database, must be accompanied by a notice containing the following elements:[17]

a whether data subjects are under legal duty to provide the requested information, or whether it is a choice they make of their own volition and consent to;

b the purposes for which the information is requested; and

c to whom the information may be onwards transferred and the purposes of such a transfer.

The PPL's notice requirement is supplemented by a requirement to obtain data subjects' 'informed consent' to processing their personal data. Under Israeli law, informed consent means a data subject's implicit or explicit consent, the subject having been provided with all information reasonably necessary to decide whether or not to consent.

The PPL grants data subjects a right to review database information that pertains to them.[18] Any individual who wishes to review the information about him or her must submit a written request to the database owner or holder. In addition, individuals who, upon reviewing information about themselves, find that it is not correct, not complete, unclear or outdated may request to correct or delete the information.

Database owners are also obligated to register their databases with the Registrar in various cases, such as where:

a the number of data subjects in the database exceeds 10,000;[19]

b the database includes information (as defined in the statute) that was not provided by the data subjects, on their behalf or with their consent;[20]

16 Section 3 of the PPL (definition of 'holder').

17 Section 11 of the PPL.

18 Sections 13–14 of the PPL and the Protection of Privacy Regulations (Conditions for Viewing Information and Procedures for Appealing Declined Requests to View), 5741-1981.

19 Section 8(c)(1) of the PPL.

20 Section 8(c)(3) of the PPL.

c the database includes 'sensitive information', defined in the PPL as information regarding an individual's personality, intimate affairs, medical or health condition, opinions or beliefs;[21] or

d The database is used for the purpose of providing others direct mailing services (as defined in the statute).[22]

Using an unregistered database whose registration is compulsory under the PPL is a strict-liability offence punishable by up to one year's imprisonment. Registration is carried out by filing a registration application and paying certain annually recurring fees. However, there are numerous nuances and potential pitfalls in the filing procedure that, if not carefully addressed, can have an adverse impact on the ability to use the database as contemplated.

iii Technological innovation and privacy law

Israeli data protection and privacy laws fail to provide clear guidance on many internet-age issues. The aged statute (dating back to 1981 with no recent significant amendments), has not been modernised to keep pace with the information age, and Israeli case law and Registrar guidelines have yet to specifically address matters such as cookies, online tracking and behavioural advertising, the 'internet of things' and 'big data'. Some issues, such as use of security and surveillance cameras in the public domain, cloud computing, and employee monitoring, have received more attention from regulators and courts.

In 2015, the Banking Supervision Department at the Bank of Israel issued guidelines to banks and credit card companies regarding the use of cloud computing services. The guidelines specify how banks and credit card companies are to go about managing the risks involved in using cloud services for data processing. The guidelines provide, among other things, that banks and credit card companies may only use cloud services if the data is stored and processed in Israel, or through a cloud service provider that adequately protects personal data pursuant to the EU Data Protection Directive.

Employee monitoring has been the subject of various labour court decisions, the most notable being a judgment delivered by the Israeli National Labor Court in 2011, which severely restricted employers' rights to monitor employees' email messages and use of IT systems at the workplace.[23]

The effective consequence of the National Labor Court's judgment is that employers may only monitor the content of their employees' email communications in corporate email accounts (but not in employees' personal webmail accounts, such as Gmail) and only if a workplace privacy policy has been instituted and prohibits employees from using their corporate email accounts for personal or private communications. The judgment also emphasises that if employees use their corporate email account for personal or private communications, even if they do so in violation of the workplace

21 Section 8(c)(2) of the PPL.

22 Section 8(c)(5) of the PPL.

23 Labor Appeal (National Labor Court) 90/08 *Isakov-Inbar v. The State of Israel, Commissioner of Women Labor* (8 February 2011).

policy, employers may still not access or use the private or personal messages in that account unless they obtain the employee's explicit, informed and freely given consent in each instance that such access is being sought, and only if the content of the message is unlawful or abusive to the employer. The judgment clarified that employers may access employee's personal email account only subject to an appropriate court order obtained in advance.

Currently pending before the Israeli National Labor Court is a dispute on whether employees can be compelled to use biometric time clocks at work, without their consent. The Attorney General of Israel has filed a brief with the National Labor Court, outlining his position, according to which in the absence of consent, forcing employees to use biometric time clocks violates employees' autonomy and invades their privacy. Furthermore, the Attorney General emphasised that employees' consent should be carefully reviewed to make sure that it was indeed informed and freely given.

iv Specific regulatory areas

In 2009, the Knesset enacted a far-reaching and highly controversial biometric ID law (the Biometrics Law).[24] The Biometrics Law seeks to institute a national database containing the biometric data of all Israeli citizens, for the declared purpose of combating large-scale loss and theft of government-issued ID cards and passports, subsequently used by criminals and terrorists. The Biometrics Law established an initial pilot period during which Israelis applying to obtain or renew their government-issued ID or passports can voluntarily choose to obtain biometric-based ID and passports, by providing their fingerprint samples and a facial photograph, to be digitally stored in a national database and on chips embedded in their newly issued ID cards and passports. Following the pilot period, biometric-based ID cards and passports will be compulsory, and all Israeli citizens will be compelled to provide their fingerprints and facial photos for storage in the national database.

The Biometrics Law, and particularly its biometric database, has raised significant concerns among privacy advocates, researchers, information security experts, computer science professionals and the state comptroller. The pilot period for the project was scheduled to end in 2015, but the Knesset voted to extend the pilot for an additional period of nine months. The Knesset's decision was passed by a narrow margin of a single vote, reflecting the controversy surrounding the law. The Israeli government has pledged to continue evaluating the project's necessity, benefits and drawbacks during this extension period, ahead of the ultimate decision whether to disband the project or transition to permanent, full-scale operation.

24 Biometric Identifiers and Biometric Data Inclusion in Identification Documents and Database Law, 5770-2009.

IV INTERNATIONAL DATA TRANSFER

Israeli law[25] severely restricts cross-border transfer of personal data originating from databases in Israel. As a starting point, such international transfers are prohibited unless the law of the destination jurisdiction abides by various data protection principles such as fair processing, purpose-limitation, data accuracy, data subjects' rights to review and correct data, and information security safeguards.[26]

Nevertheless, Israeli data transfer regulations go on to provide certain 'safe-harbour' exceptions that permit cross-border transfer of personal data even if the data is transferred to jurisdictions whose laws do not mandate the required principles.[27] For instance, cross-border transfer of data may be permissible if:

a the data subject has consented to the transfer; or

b the data is transferred to an affiliate controlled by the corporation from which the data transfer originates; or

c the data is transferred to a person contractually bound to comply with the same conditions for possession and use of personal data that apply to a database in Israel, *mutatis mutandis*; or

d the data is transferred to a jurisdiction that is either:
- a party to the European Convention for the Protection of Individuals with Regard to Automatic Processing of Sensitive Data; or
- a country recognised by the European Commission as ensuring an adequate level of personal data protection pursuant to the EU Data Protection Directive.[28]

Following the recent judgment of the Court of Justice of the European Union (CJEU) striking down the US-EU Safe Harbor Framework, ILITA published a statement clarifying that Safe Harbor can no longer be relied on as a legal basis under Israeli law for cross-border transfer of personal data from Israel to Safe Harbor-certified US entities. Prior to the CJEU judgment, ILITA held the position that the US-EU Safe Harbor programme could be utilised for such cross-border transfer of personal data, under the regulation's rubric of 'a country recognised by the European Commission as ensuring an adequate level of personal data protection pursuant to the EU Data Protection Directive'.

Nevertheless, Israeli data transfer regulations set forth additional, conjunctive requirements.[29] These require that the database owner from which the data transfer originates bind the foreign data recipient to a written statement according to which the

25 Protection of Privacy Regulations (Transfer of Data to Databases Abroad) 5761-2001. An unofficial translation of these regulations is available at: www.justice.gov.il/NR/rdonlyres/6A5EC09A-BDBC-419F-8007-5FD6A6B8E0A5/18342/PrivacyProtectionTransferofDataabroadRegulationsun.pdf.

26 Regulation 1 of the Protection of Privacy Regulations (Transfer of Data to Databases Abroad).

27 Regulation 2 of the Protection of Privacy Regulations (Transfer of Data to Databases Abroad).

28 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

29 Regulation 3 of the Protection of Privacy Regulations (Transfer of Data to Databases Abroad).

recipient guarantees that it employs sufficient means to ensure the privacy of data subject and that the personal data will not be further transferred onwards to any other person or entity, whether in that same country or another country. Thus, Israeli law effectively prohibits any onward transfer of personal data by the foreign recipient to another ('second-tier') person or entity downstream. This prohibition clearly raises significant problems, particularly for international corporations seeking to process their employee or customer data. Unfortunately, the Israeli data transfer regulations prescribe this in no uncertain terms, and regrettably, there is no Israeli case law or Registrar guidelines that might clarify whether this 'flat ban' can be somehow relaxed.

Israeli data transfer regulations also raise particular problems with respect to cloud services, because cloud services typically process data at various servers spread throughout the globe, rather than confine it to servers located in a single jurisdiction.

Israeli law has not adopted mechanisms comparable to EU law's 'standard contractual clauses' or 'binding corporate rules'. Nevertheless, since 2011 Israel is recognised by the European Commission as providing an adequate level of protection for personal data pursuant to the EU Data Protection Directive.[30]

V COMPANY POLICIES AND PRACTICES

Organisations that engage in collecting and processing personal data from consumers through the internet or mobile apps, can typically comply with the PPL's notice and informed consent requirement by having a properly drafted and properly delivered privacy policy.

Pursuant to the aforementioned Israeli National Labor Court judgment, employers seeking to engage in any form of employee monitoring are required to institute a balanced workplace privacy policy. The policy needs to establish the employer's guidelines on acceptable and prohibited uses of corporate email accounts and other IT resources available to employees at work, as well as information on the nature and scope of measures being used by the employer to monitor its employees (including surveillance cameras). The policy's guidelines and substance must conform to the principles of transparency, proportionality, legitimate purpose and purpose-limitation (as set forth by the court), and employers must obtain employees' written consent to their policies.

The Registrar has published guidelines imposing a stringent set of requirements on organisations seeking to commission outsourcing services to process personal information (the Outsourcing Guidelines).[31] The Outsourcing Guidelines require commissioning organisations to perform certain pre-engagement due diligence reviews; enter into a written agreement with the data-processing services provider, and impose numerous

30 Commission Decision of 31 January 2011 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data, Official Journal of the European Union, L27 Volume 54, page 39 (1 February 2011).

31 Guidelines No. 2/2011 of the Registrar of Databases, 'Use of outsourcing services for processing personal information'.

contractual obligations upon it. Issues outlined in the Outsourcing Guidelines include establishing information security measures; service providers' insurance coverage; ban on transferring to others, or 'co-mingling', data obtained by virtue of an engagement with the commissioning organisation; and the commissioning organisation's right and the Registrar's authority to audit the service provider.

VI DISCOVERY AND DISCLOSURE

The Israeli Wiretap Law, 5739-1979 authorises investigative and security authorities to surreptitiously obtain the content of communications such as telephone calls, internet traffic data and email messages, in real time (communications in transit), for national security purposes or for the purpose of preventing and investigating serious crime. Wiretaps sought for national security purposes are only subject to the prior approval of the Prime Minister or Minister of Defense. They are not subject to judicial review or court approval. Wiretaps sought for preventing and investigating serious crime are subject to court approval, which in exceptional cases can be sought after the fact.

The Israeli Telecom Data Law[32] provides police and various other investigative bodies with the authority to apply to the court of lowest instance in Israel to seek a comprehensive order to surreptitiously receive metadata (but not the content) of telecommunications, for the purpose of search and rescue, investigating or preventing crime, or seizing property. If metadata is required urgently and a court order cannot be obtained in time, such metadata may be obtained for a limited period of 24 hours, without a court order, subject to approval by a senior police officer.

Apart from the Israeli Telecom Data Law, the statute governing the operation of the Israeli Security Agency (colloquially known as 'Shabak' or 'Shin Bet') grants the Prime Minister sweeping powers to order that metadata and non-real time communications (traffic data at rest), be retained by telecom providers and surreptitiously made available to the Israeli Security Agency, without court approval or judicial review.[33]

Section 13 of the Communications Law (Telecommunication and Broadcasts), 5742-1982, provides that the Prime Minister may order telecom service providers to render services to police, security agencies and intelligence agencies, and to have the providers install devices, take measures or adapt their facilities to assist the authorities in carrying out their roles and objectives. Such orders have been issued and they apply to every major Israeli telecom provider, though the substance of the orders have not been disclosed.

The Regulation of Security in Public Bodies Law authorises the Israeli Security Agency to issue binding directives to organisations operating critical infrastructures on matters related to information security and cybersecurity, and inspect such organisations'

32 Officially known as the Criminal Procedure Law (Enforcement Powers – Communication Data), 5767-2007.

33 Section 11 of the General Security Service Law, 5762-2002. An unofficial translation of the law is available at: https://www.knesset.gov.il/review/data/eng/law/kns15_GSS_eng.pdf.

compliance with those directives.[34] Organisations subject to this regime include telecom and internet providers, Israel Railways, the Israel Airports Authority, the Tel Aviv Stock Exchange, utility companies and others.[35] The Israeli Security Agency's powers in this respect are exercised by its subunit named the National Information Security Authority.

VII PUBLIC AND PRIVATE ENFORCEMENT

i Enforcement agencies

Israel's data protection and privacy enforcement agency is the Registrar of Databases, operating within ILITA at the Ministry of Justice. The Registrar is vested with investigative and audit powers. Pursuant to the PPL, Registrar inspectors can conduct announced or unannounced audits at premises where databases are being administered, collect evidence and seize computers. The Registrar is also authorised to impose administrative sanctions in several forms: mere declarations of fault, fines, and suspension or revocation of database registration. The Registrar discloses succinct descriptions of some of its enforcement activities, on its website.

Criminal indictments in the realm of data protection and privacy are handled by the Attorney General.

ii Recent enforcement cases

In recent years, the Registrar has been focusing enforcement efforts on data brokers that unlawfully engage in data enhancement services using government-administered databases that have been leaked: the population database (containing detailed information of all Israeli residents and citizens, including the deceased) and the voter roll database.

Those involved in the original misappropriation of the population database were indicted, convicted and sentenced. Recently, a data broker was found by the Registrar to be using the leaked population database for its offerings of data services for marketing purposes. The data broker was fined and ordered to discontinue its business. ILITA also took an aggressive and questionable approach of contacting the data broker's numerous clients, which span virtually all sectors of the Israeli economy, demanding that they promptly cease using the data obtained from the broker and destroy it.

Other enforcement activities made public in recent years have dealt with data breaches associated with violations of the statutory duty to employ information security measures, violations of duties regarding direct mailing activities, and use of databases for purposes inconsistent with their registered purpose. These have resulted in declarations of fault, and some also in fines.

34 Sections 10 and 15 of the Regulation of Security in Public Bodies Law, 5758-1998.

35 Schedule 4 to the Regulation of Security in Public Bodies Law.

iii Private litigation

The PPL provides for a civil cause of action for invasion of privacy committed through one of the eventualities enumerated in Chapter 1 of the PPL. Thus, Chapter 1 of the PPL is a vehicle through which plaintiffs can sue companies that use personal data in ways that data subjects did not consent to.

Available remedies include actual damages for proven injury or harm, injunction and statutory damages (nowadays, up to US$30,000) that address common situations in which plaintiffs face difficulties in establishing actual damages or injury.[36] Invasion of privacy committed in the context of relations between businesses and consumers establishes grounds for class action.

Overall, other than lawsuits on prohibited spam communications (a matter governed by laws extrinsic to data protection legislation), private litigation on data protection and privacy is not common in Israel.

VIII CONSIDERATIONS FOR FOREIGN ORGANISATIONS

Questions on the applicability of the PPL in cases that involve foreign (non-Israeli) factors, is an unsettled area of law. For instance, Israeli privacy and data protection law remains unclear as to whether merely processing personal data collected online from Israeli web users, is sufficient to subject the data-processing activities to Israeli data protection laws, if those activities are conducted exclusively outside Israel, by an entity incorporated outside Israel with no other nexus to Israel. Contrarily, the applicability of the PPL in cases involving collection of personal data from Israeli employees is far less questionable, regardless of the jurisdiction in which the employer is situated. At any rate, to date, ILITA has not conducted enforcement activities with respect to such data handlers and the Registrar has not officially stated its position.

In cases where the PPL applies to data-processing activities, use of data servers physically situated outside Israel is subject to the regulations governing cross-border data transfers, as outlined above.

IX CYBERSECURITY AND DATA BREACHES

The PPL imposes a set of requirements on the 'manager' of a database, who is 'an active officer in an organisation that owns or holds a database, or such other person that said officer has authorised to act as such in this regard'.[37] The manager, along with the database owner, its holder[38] and the organisation's information security officer,[39] are responsible

36 Section 29A of the PPL.

37 Section 7 of the PPL.

38 Section 17 of the PPL.

39 Section 17B(b) of the PPL. Any person or entity who holds at least five databases must appoint a 'suitably trained person' to be in charge of information security. The PPL does not

for 'protecting the integrity of data and safeguarding it from unauthorised exposure, use or copying'.[40] This is the primary and almost exclusive responsibility of the manager pursuant to the PPL.

The PPL's Data Possession Regulations[41] address this matter in greater detail, but they are somewhat archaic, having been promulgated in 1986 (and slightly amended in 2005). They do not purport to exhaust all measures that the manager should employ to secure the information, and specify only a partial list of topics that the manager is entrusted with.

Among other things, the Data Possession Regulations require 'implementing physical safeguards', 'establishing database access privileges', and 'employing reasonable security measures, commensurate with the sensitivity of the information'.

In 2012, the Registrar proposed a draft amendment to the Data Possession Regulations. The draft proposed much more expansive information security arrangements and procedures regarding databases as well as broader enforcement powers to investigate, issue cease-and-desist orders and impose elevated administrative fines. However, to date, no real progress has been made with the actual enactment of the amended Data Possession Regulations and there is no solid assessment of the expected timeline for such an enactment.

In 2015, the Banking Supervision Department at the Bank of Israel issued a circular on cyberdefence management at banking corporations and credit card companies.[42] One of the circular's operative sections requires that banking corporations and credit card companies appoint a cyberdefence manager and define the board of directors' responsibilities in this realm. The circular specifies that banking corporations are expected to regularly identify and evaluate cyber threats and risks, and details the requirements for an effective process for identifying and evaluating cyber risks. The circular also points out that banking corporations ought to continuously examine the effectiveness of the various cyberdefence controls that they have established – using tools such as vulnerability reviews and controlled-intrusion tests.

The Banking Supervision Department at the Bank of Israel indicated that it plans to follow up with another directive regarding information security at banking corporations.

This year, the Israeli government began establishing a national authority for cyberdefence. The executive decision on the establishment of the national cybersecurity authority prescribes its primary roles, as follows:

a manage, control, and carry out the overall, nationwide operational efforts to protect cyberspace;

---

elaborate on the required qualifications of the security officer, other than him or her being a 'suitably trained person'. Even though the PPA does not expressly impose this obligation on the database manager, it is undoubtedly the manager's duty to appoint such as person.

40 The definition in Section 7 of the PPA.

41 Protection of Privacy Regulations (Conditions for Possessing and Protecting Data and Procedures for Transferring Data between Public Bodies), 5746-1986.

42 An English version of the circular is available at: www.boi.org.il/en/BankingSupervision/LettersAndCircularsSupervisorOfBanks/Curculars/h2457_en.pdf.

b operate a national, economy-wide Computer Emergency Response Team (CERT);
c strengthen and reinforce the economy's resilience, through preparatory measures and regularisation;
d design and implement a national cyberdefence doctrine; and
e perform such duties as the Prime Minister may determine, consistent with the authority's designated mission.

X OUTLOOK

An overhaul to the Credit Data Services Law is in the pipeline for the coming year, with a pending draft bill seeking to significantly expand the scope and availability of creditworthiness data about individuals, for the purpose of enhancing competition in the credit market.

The Israeli Ministry of Justice and the National Cyber Bureau are planning to prepare a draft bill for a cyberdefence law, and evaluate the need for additional legislative amendments in the cybersecurity domain.

It remains to be seen whether the EU's proposed General Data Protection Regulation will have a significant impact on the Israeli data protection landscape. Likewise, it remains to be seen whether the Israeli government and legislature will engage in the much-needed modernising overhaul of the PPL.

Appendix 1

ABOUT THE AUTHORS

HAIM RAVIA

Pearl Cohen Zedek Latzer Baratz

Haim chairs the internet, IT and copyright group at Pearl Cohen. Nominated by *Who's Who Legal* as one of the leading lawyers in technology, media and telecommunications since 2010, he deals extensively with data protection and privacy, computer and internet law, IT contracts, copyright, electronic signatures, and open-source software. Haim was a member of the public commission for the protection of privacy, acting under the auspices of the Ministry of Justice by virtue of the Protection of Privacy Law, and was part of a governmental team that re-examined the Israeli law pertaining to databases. Haim frequently advises insurance and financial companies, telecommunications carriers and health organisations on privacy and data protection issues, including representation of clients before the Israeli Law, Information and Technology Authority (ILITA).

DOTAN HAMMER

Pearl Cohen Zedek Latzer Baratz

Dotan is a senior associate attorney in the internet, IT and copyright group at Pearl Cohen. Dotan regularly advises Israeli and multinational corporations on the intricacies of Israeli data protection and privacy laws. Having completed his academic degree in computer science at the age of 19, and later working as a software developer and a technological project leader, Dotan also counsels clients on software and 'software as a service' (SaaS) user agreements and licensing, digital (electronic) signatures, copyright issues, open-source matters and other aspects of the law relating to computers, the internet, and information technology.

PEARL COHEN ZEDEK LATZER BARATZ
5 Shenkar Street
Herzliya 4673339
Israel
Tel: +972 9 972 8000
Fax: +972 9 972 8001
hravia@pearlcohen.com
dhammer@pearlcohen.com
www.pearlcohen.com