Thinking Out Loud About Cloud

A deep dive in the state of cloud computing in Israel.

October 23, 2017

Yoheved Novogroder-Shoshan

KEYWORDS

2016 was a watershed year for global privacy, with major developments taking place in the area of personal data regulation worldwide. Surprisingly, while Israeli companies are leaders in technological innovation, in certain key respects Israeli privacy laws that purport to regulate those innovations are old, technologically irrelevant and devoid of meaningful guidance to industry as to how the laws are to be applied in the real world.

This dichotomy of technological advancement accompanied by regulatory antiquation is particularly striking in the cloud computing arena. Israeli companies are both leading providers

of cloud-based services and avid consumers of such technologies. Israel's data protection laws are in need of modernization to accommodate the cloud-based services that are a mainstay of the Israeli business environment. Lack of regulatory guidance challenges both providers of cloud-based services as well as Israeli businesses seeking to use these services.

Cloud Services in Israel

Israeli companies offer a wide range of cloud-based services, including in areas of security, IT management, mobile applications, quality solutions, business intelligence, enterprise solutions (such as CRM, ERP, collaborative applications, HR management applications), industry-specific solutions and well as enablement or management solutions such as security and performance. In January, Oracle demonstrated faith in the Israeli cloud technologies ecosystem with the creation of an Israeli start-up accelerator focused on cloud innovation, the second such center to be founded globally.

Legal Framework

Understanding the laws applicable to Israeli providers and consumers of cloud-based technologies requires a basic familiarity with the structure and content of the Israeli privacy regime. Israel was an early adopter in the area of privacy regulation, and has had a national data protection law for over thirty-five years. The foresight of Israeli legislators, while admirable, was not followed by significant updates to the law in several key areas, yielding a data protection regime that is ill-suited to the cloud-based technologies heavily relied upon by the Israeli technology and leaves Israeli based suppliers of such solutions without much-needed guidance.

Israel’s primary data protection law is the “Protection of Privacy Law-1981” also known as the Privacy Law. The Privacy Law is supplemented by various regulations as well as sector-specific laws that apply medical, genetic, financial, credit, and other information. Underscoring the primary importance ascribed to privacy by Israeli legislators, the Privacy Law's protections are supplemented by the quasi-constitutional “Basic Law: Human Dignity and Freedom,” also known as Basic Law, which recognizes the right to privacy as a as a fundamental human right. The Basic Law states, ‘Every person is entitled to privacy and to the confidentiality of his life’ and ‘there shall be no infringement of the confidentiality of a person’s conversations, correspondence and writings’.

The Israeli Law Information and Technology Authority (ILITA) has functioned as Israel’s data protection authority since 2006 and serves as the Registrar of Databases (Registrar). ILITA has issued a number of detailed directives, which at the minimum, are indicative of ILITA's interpretation of applicable law and are predictive of possible future ILITA enforcement activities. During the early years following its formation, ILITA had a higher level of engagement and communication with local industry, making itself available at public forums and providing informal indications of its view of existing law and enforcement priorities; this activity has waned somewhat in recent years.

Privacy and Databases

The Privacy Law includes general privacy provisions as well as provisions specifically applicable to databases. The Privacy Law's privacy provisions prohibit an infringement of the privacy of any person without that person's consent, provide for both civil and criminal liability for an infringement of privacy, and identify a range of activities which, if carried out without consent, constitute privacy breaches.

"Person" under the Privacy Law only includes natural persons. Thus, while the Privacy Law's privacy, data protection, and database provisions do not by their terms apply to corporations or other legal entities, under case law corporations are entitled to limited privacy rights.

In addition to the privacy provisions described above, the Privacy Law provides a detailed regime for the regulation of databases. The Privacy Law defines a database as "a collection of data, stored by magnetic or optical means and intended for computing processes," with certain databases not intended for commercial use exempted from the definition.

"Data" is defined in the Privacy Law as details regarding a person's personality, personal status, private affairs, state of health, economic situation, professional qualifications, opinions, and faith. The Israeli Supreme Court interprets the term data broadly, and the term "private affairs" is often construed by Israeli courts as encompassing various types of personal information that are not specifically mentioned in the definition above. Thus Israeli Supreme Court decisions have held that a person's address, telephone number, bank account information, national ID number, and IP address are all deemed as data under the Privacy Law.

Since "person" under the Privacy law refers to natural persons, collections of data that do not relate to a "person" are not deemed "databases" under the law and are not subject to the Privacy Law's database provisions. As such, a collection of data that contains information solely regarding corporate entities would not be deemed a database under the Privacy Law. However, if the collection of data includes data regarding individuals associated with those entities, or information regarding other individuals, the collection of data would be deemed a database for purposes of the Privacy Law. Most collections of data used for commercial purposes — for example cloud-based customer relationship management (CRM) solutions favored by Israeli businesses — are likely to be subject to this database framework even where most or all customers corporate entities and not individuals.

As mentioned above, the Israeli legal regime provides certain challenges when applied to the cloud context. Certain of these are discussed below.

Cloud Challenge #1: Territorial Application; When is a Database Subject to Israeli Database Laws?

Unlike the EU General Data Protection Regulation and certain other national data protection laws, the Privacy Law and attendant regulations are silent on the law's territorial scope. To date, ILITA has not issued guidance on this point. While for many years ILITA has indicated that it is

preparing guidance as to application of Israeli law in the cloud computing context, as of the date of this article no such guidance has been issued and the timing for release of such guidance is unclear.

In the absence of firm guidance from the regulator, it is possible that four factors would be relevant to the question of whether a database stored in the cloud is subject to Israeli law:

1. Server location: Are the servers physically located in Israel?
2. Location of database owner/controller: Does an Israeli company hold legal authority to direct access to and use of the database, or is the company's management based in Israel?
3. Location of processing: Are the database administrator or individuals who actively process data on a regular basis based in Israel?
4. Data subjects: Are there Israeli data subjects?

If this four-factor test were indeed to be applied, when an Israeli entity engages a cloud based service provider the resultant database created would be subject to Israeli legal protections regardless of where the cloud service provider is located.

The situation is somewhat more complex when the provider of cloud-based services is located in Israel. Under that scenario, factors (1) and (3) may or may not be met, depending on where servers are located and where processing activities are performed. Similarly, factors (2) and (4) may or may not be satisfied, depending on the location of the customer and data subjects. The Privacy Law provides providers and consumers of cloud-based services virtually no guidance as to the key question of territorial application of Israeli database laws and responsibilities there under.

Cloud Challenge #2: Data Export Restrictions

Israeli law restricts international data exports, and 'subsequent transfers' from data recipients outside Israel to others are strictly prohibited. The extent to which these data transfer restrictions apply in the cloud context is not clear. Consider the case of an Israeli-based cloud service provider — when the provider's non-Israeli customers use their own data stored on servers outside of Israel, have these entities violated Israeli database laws? ILITA has not addressed these questions. Such application of the data export regulations would appear to be illogical.

One advantage held by Israeli clouds services providers is the EU adequacy ruling, issued in 2011 and designating Israel’s domestic law as guaranteeing an adequate level of protection for personal data. This inclusion on the EU 'white list' of adequate countries enables the transfer of personal data from the EU to Israel without special arrangements such as standard contractual clauses or binding corporate rules; for purposes of EU privacy law, data transfers from the EU to Israel are treated as substantially equivalent to transfers from one EU country to another.

Shortly following the EU adequacy ruling, the then-incumbent Israeli Database Registrar publicly stated that ILITA would not enforce data transfer regulations for data exports to EU-based data owners who had transferred data to Israel. This statement was not formalized in

official guidance. We would hope that ILITA would take the same approach with respect to non-Israeli consumers of cloud services provided by Israeli companies regardless of where the consumers are located.

Cloud Challenge #3: Database Registration

Israel has a mandatory database registration requirement that poses particular challenges to Israeli providers of cloud-based services. Database owners must register databases with the Israeli Database Registrar ("Registrar") where any one of the following conditions is met:

- The database contains data about more than 10,000 people
- The database contains sensitive material
- The database contains data about natural persons not provided by them, on their behalf or with their consent
- The database belongs to a public body
- The database is used for direct mail services

Since all financial data, health data, or other data regarding a person's personality, private affairs, opinions or faith, and government-issued personal identification numbers are all considered sensitive data, the registration requirement applies to many databases that do not meet the 10,000 data subject threshold.

The registration requirement raises a number of questions. For example, when an Israeli company provides cloud-based storage or processing services, are non-Israeli customers obligated to register the relevant databases in Israel? Applying the registration requirement in this manner would destroy international demand for these services.

In addition, while database registration is the responsibility of the database owner, Section 8(a) of the Privacy Law provides that it is prohibited to "hold" a database that must be registered pursuant to Section 8 of the Privacy Law unless the database has been so registered or a registration application has been submitted and no response has been received within the statutory period.

ILITA has taken an expansive view on what entities are considered database "holders" and has indicated that entities providing storage services are deemed database holders for purposes of the Privacy Law. Are Israeli 'storage as service' cloud providers in violation of the law if their non-Israeli customers have not registered the stored databases in Israel in accordance with Israeli law? The Privacy Law does not provide guidance on this point. The requirement to register these databases would seem to be unduly burdensome and onerous, and inconsistent with the rationale behind the registration obligation. While a draft law currently pending before the Israeli parliament would abolish the database registration obligation for the vast majority of databases, the questions above would remain with respect to the narrower class of registerable databases.

Admittedly some of the challenges described above are not unique to Israel. It has been argued that the EU General Data Protection Regulation which will become effective in May 2018

presents significant challenges to EU-based cloud service providers. What is clear is that the world has changed dramatically in the 35 years since the Israeli Privacy Law was enacted. For the befit of the Israeli cloud service ecosystem and the myriad of Israeli companies utilizing cloud based services for HR management, ERP and other services, the time has come for ILITA to provide much-needed guidance on how these services may be provided and used in compliance with Israeli laws.

The online version appears here