from the servers, and read on their computer screens in Canada, is not located in Canada."

The Court also concluded that the extra-territorial application of Canada's Income Tax Act was not a significant issue on the facts in the case. It noted that the agreements with eBay Canada expressly provide that they may disclose confidential "eBay System Information" (which included information about PowerSellers) which "is required to be disclosed by order of any court". Nor, noted the Court, did the Income Tax Act provision oblige a person outside Canada to do anything.

The Federal Court of Appeal decision is only a month old, so its value as a precedent in other jurisdictions is not yet clear. However, it has offered some guidance on the status of personal data about individuals from one country held on the servers of a company abroad, but accessible from the first country.

• *Further information:* eBay Canada Ltd. v. Canada (National Revenue), *2008 FCA 348: http://decisions.fca-caf.gc.ca/en/2008/2008fca348/2008fca348.html.*

AUTHOR

Eugene Oscapella is a Consultant at Privacy Laws & Business, Canada
eugene.oscapella@privacylaws.com

Israel's new anti-spam law: seller beware

Direct marketing requires affirmative consent. By Omer Tene

Effective 1 December 2008, Israel's new anti-spam law is set to stir change in the way companies communicate with existing and potential clients. The new law, enacted last May as the Telecommunications Act (Telephone and Broadcast) (Amendment No. 40), 2008, is modeled after the European Electronic Communications Privacy Directive (2002/58/EC). It applies to businesses sending direct marketing messages by electronic means, such as by automated calling systems, fax, email, and text messages (SMS and MMS). It imposes stiff civil and criminal penalties on infringing companies and therefore warrants technical, organisational and commercial readiness.

The Act prohibits the transmission of "advertising material" by electronic means without the recipient's prior explicit consent, which must be expressed in writing, including an electronic message or a recorded conversation (Section 30A (b)). Hence, direct marketing is subjected to a regime of affirmative opt in consent. "Advertising material" is defined as "a commercially distributed message intended to offer for sale a good or service or otherwise promote a monetary expenditure" (Section 30A(a)).

The Act provides two important exemptions: first, advertisers may contact a business (as opposed to individual) recipient once to solicit consent for future communications (Section 30A(b)); second, advertisers may transmit advertising material to an individual recipient if (a) they obtained the contact details of the recipient in the course of a sale or negotiations for the sale of a product or service and notified the recipient at that time that those details would be used for electronic transmission of advertising material; (b) the recipient has been given a simple means (free of charge except for the cost of transmission) of refusing to accept additional advertising material; and (c) the advertising material relates to a similar product or service (Section 30A(c)). The Act thus provides a "soft opt in" rule for existing customers.

> Advertisers are subject to a fine of an amount up to 202,000 New Israeli Shekels (more than $50,000).

The Act regulates not only the means of transmission but also the content of advertising messages. Under the Act, an advertising message must be clearly labeled as such, using the word "advertisement" at the beginning of the message or, in case of an email message, the subject line. In addition, an advertising message must specify the name and contact details of the advertiser as well as the recipient's right to notify the advertiser at any time and by reasonable means of his or her refusal to receive additional messages (Section 30A(e)). To avoid exceedingly long messages, the senders of SMS must specify only their name and contact details.

The Act imposes liability not only on the party actually sending the advertising message but also on any party (a) whose name or contact details appear in the message for the purpose of purchasing goods or services; or (b) whose business or purposes may be promoted by the message (Section 30A(e)). Companies working with third party advertisers or direct marketing services must therefore ensure compliance by their service providers in order to avoid potential liability for illicit messages sent on their behalf. The Act explicitly exempts from liability telecommunications service providers which serve as "mere conduits" in the transmission of an advertising message.

By Israeli standards, the penalties under the Act are harsh. Advertisers are subject to a fine of an amount up to

202,000 New Israeli Shekels (more than $50,000) for each message sent in violation of the Act, or up to 67,000 NIS (more than $17,000) for messages not containing the requisite content (Section 30A(f)). Furthermore, the Act imposes personal liability on directors and officers, including marketing managers, of infringing advertisers in an amount up to 67,000 NIS (more than $17,000) (Section 30A(h)). Violation of the Act constitutes not only a criminal offence but also a civil tort (Section 30A(i)). Recipients may be awarded statutory damages in an amount up to 1,000 NIS (more than $250) for each infringing message they received (Section 30A(j)). Moreover, recipients of infringing messages may bring a class action lawsuit under the Act.

Advertisers must ensure compliance not only with the Act but also with the direct marketing provisions of the Privacy Protection Act, 1981 ("PPA"). Interestingly, the relevant PPA provisions, which have not been eclipsed by the current amendment, provide an opt out regime for direct marketing (Section 17F of the PPA). Consequently, advertising by means other than automated calling, fax, email, or text messages (for example telemarketing or regular mail) remain subject to an opt out regime.

In addition, since direct marketing activities necessitate the use of customer lists and databases, advertisers must comply with the PPA provisions on data protection. Under Section 8 of the PPA, a database must be registered with the Database Registrar if it contains data used for direct marketing services or data which have been collected from third parties. In addition, to prevent potential law suits, advertisers would be well advised to maintain a customer database documenting each customer's consent to receive advertising messages. Advertisers should also consider separating databases of existing from potential customers as well as databases of customers who have given consent to receive advertisements from those who partially or wholly withheld consent.

Certain of the Act's definitions remain rife with ambiguity. For example, it is not clear what constitutes "a commercially distributed message" under the Act. Is the test technical, assessing the number of targeted recipients, or contextual, examining the contents of the message? For example, a message by a store owner to a single customer telling her of a new product and asking her to visit the shop may not be regarded as "commercially distributed" under a technical test (since there is no mass distribution) but would be regarded as such under a contextual test. Conversely, a message sent to thousands of recipients to solicit contributions to a charity would be regarded as "commercially distributed" under a technical test but not under a contextual test. Similar uncertainty may surround dual-purpose messages containing both professional and commercial material, such as newsletters featuring banner ads or the contact details of a lawyer or accountant.

An additional provision likely to raise questions is the business recipient exemption. Specifically, which rules will apply to unsolicited marketing messages sent by email to individual employees of a corporation, where such messages promote goods and services that are clearly intended for their personal or domestic use? On one hand, the statutory purpose of the Act would be defeated if an advertiser were permitted to send advertising messages to each employee of a corporation under the guise of a business mailing. On the other hand, how could an advertiser conceivably send a message to a business recipient without targeting an individual employee?

Until these matters are resolved by the courts, clients are advised to err on the side of caution, to avoid unnecessary litigation and sanctions.

AUTHOR

Dr Tene is a legal consultant and an Associate Professor at the College of Management School of Law, Rishon Le Zion, Israel. omer.tene@bezeqint.net
www.omertene.com

Irish data breach law?

The Irish Minister for Justice, Equality and Law Reform, Dermot Ahern, on 28 November set up a group to consider mandatory data breach notification legislation. The group is chaired by the former Secretary General of the Irish Department of Finance, Eddie Sullivan. Billy Hawkes, the Data Protection Commissioner, is also in the group. The chief focus of the examination will be whether changes are required to Data Protection legislation to deal with data breaches, according to a 31 October statement of the Data Protection Commissioner[1]s Office.

The group will examine whether the introduction of mandatory data breach notification is necessary, as well as any related penalties.

Minister Ahern said: "Given recent experiences, there is an understandable concern in the public mind at reports of [personal] data being lost or mismanaged. Various suggestions have been made as to how Data Protection legislation ought to be amended to address these concerns, and I intend to get a broad assessment of these complex issues and the possible impact of any changes. I am asking the Group to make early interim recommendations if they consider there are matters that can be dealt with expeditiously … I expect that the Group will consult widely as part of their deliberations and I look forward to their report. I trust that the innovative linking of the public consultation process with a Regulatory Impact Assessment will lead to a well-structured analysis of a complex area and ultimately to a robust outcome".

On 3 November 2008, the Bank of Ireland (BOI) notified the Data Protection Commissioner of the loss of a memory stick containing customers' personal details. According to a statement of the Data Protection Commissioner the memory stick contained only "relatively limited" personal data.

Israeli database bill introduced

A bill to create a national biometric database was introduced in the Knesset (the Israeli parliament) during the last week in October. It would require fingerprints and digital photos on Israeli identification cards and passports, which would be included in a national database.