Banishing spam

New crackdown to include all e-messages, experts say

BY DREW HASSELBACK, FINANCIAL POST JANUARY 6, 2011

Change is afoot for those who rely on email for marketing.

The federal government has passed a law that will bar the sending of unsolicited email or spam.

Bill C-28, the Fighting Internet and Wireless Spam bill, was granted royal assent in December and should be in force by summer, lawyers say. This gives corporate counsel several months to begin talks with IT departments to ensure their companies are in compliance.

The legislation is supposed to apply to any electronic message sent over any means of telecommunication, and this should be broad enough to include not just conventional email, but also things such as postings on Twitter or Facebook.

Indeed, Rebecca Chan, partner with Borden Ladner Gervais LLP in Toronto, says corporate counsel should be raising the matter with any staff who deal with social media. "The way it's drafted is technology neutral. So it can pick up other forms of mass communication."

The main thing companies need to ensure is that they are only sending emails to Canadians with their consent. Explicit consent is the easiest approach. When companies collect consumer data, they should make sure they're being forthright about asking consumers whether they want to receive emails in the future. Any messages sent from then on need to contain information on how the consumer can unsubscribe from the list.

The act does allow for implicit consent in narrow circumstances. These include situations where the customer has an existing business relationship with the company, or where recipients freely publish their email addresses on the Web without a statement warning that unsolicited messages are unwelcome.

The act also includes some specific exemptions. For example, companies are allowed to send out unsolicited emails with information about product upgrades or warranties.

Another key provision companies should be aware of is a bar on the installation of programs on consumers' computers without their consent. This is designed to limit the spread of spyware or malware.

Businesses need to ensure that any third-party contractors they hire for marketing campaigns are also in compliance with the new rules. You can't outsource your marketing, then plead ignorance if your contract provider runs afoul of the law.

The act makes it an offence to send false or misleading electronic messages. This refers not just to the content of the message, but also to any attempt to mask the sender's identity or location. These provisions are designed to attach to emails that pitch scams. This should only concern reputable companies if their business plans involve connecting heirs with the oil fortunes accumulated by their recently deceased Nigerian uncles.

The CRTC is responsible for enforcing the act. Penalties can reach up to $1-million for individuals and $10-million for organizations.

An obvious question is whether the law will succeed in reducing or eliminating the amount of unwanted email flowing into your inbox. Unfortunately, the law will have to operate for a few years before anyone can answer that one effectively.

"It raises expectations, but like the Do Not Call List, one wonders," says David Elder, a counsel with Stikeman Elliott LLP in Ottawa. "Certainly the more reputable companies are always going to try to respect the law."

The National Do Not Call List managed by the CRTC is supposed to protect Canadians from receiving unwanted telemarketing calls. Critics, such as University of Ottawa professor Michael Geist, have called it a disaster.