

Infinity Direct

What You Need to Know About Canada's New Anti-Spam Bill

In an effort to strengthen protection against problems like email spam, spyware, and phishing scams, Canada recently introduced the Electronic Commerce Protection Act, also referred to as the ECPA or Bill C-27. If the bill becomes law, which we believe could occur sometime early 2010, it will cover any "commercial electronic message" which is sent from, routed through, or accessed within Canada. The following is a summary of our understanding the ECPA as it stands today, including our opinion on how it could affect email marketers if the bill is enacted into law. It is not legal advice. As with all legislation, US or Canadian, you should seek professional legal advice if you have any concerns about how this will affect your business.

Permission is Required The ECPA prohibits the sending of commercial email without prior permission from the recipient; in other words, you must only send emails to people who have signed up to receive those specific emails. Note this differs from the US CAN-SPAM law, which in most cases does not require advance permission to send emails. While there are provisions for prior implied consent included in the ECPA as long as a relationship can be established between the sender and the recipient, these rules are more complex - and our BlueHornet Solution permission policies may ultimately supersede them. We'll provide updates and additional detail as the bill progresses.

Unsubscribe Processes The ECPA requires that all commercial email messages must include an unsubscribe mechanism which will be active for at least 60 days after the message was sent. It also allows 10 days to act on any unsubscribe requests. Compare this to CAN-SPAM, where the unsubscribe mechanism must be active for 30 days and unsubscribe requests must be handled within 10 business days.

Our BlueHornet Solution will immediately unsubscribe any request via our standard unsubscribe link. However those individuals requesting to unsubscribe via other methods (e.g., hitting reply or via postal mail) require action on your part to manually unsubscribe these requests. If you're not using a consistent unsubscribe link you may need to change your process to meet ECPA requirements.

Maintain a "Clean" Database The ECPA requires email marketers to regularly remove bounced/marked as spam email addresses from your database. Our BlueHornet Solution's bounce processing will automatically handle the former, and our feedback loops will help address the latter--for ISPs who offer feedback loops. And remember, complaints that are sent directly to you via email or postal mail will require action on your part.

Transactional Messages CAN-SPAM exempts transactional messages from regulation, assuming a recent transaction is the "primary purpose" of the message. In comparison, any message that contains promotional or marketing content--even if minimal--must comply with ECPA rules. This is one part of ECPA that is most likely to require you to evaluate your current practices. Again, as we obtain updates, we'll make sure to pass them on so you can ensure you're in compliance once the bill is passed.

Individuals Can Sue Violators The Canadian bill contains provisions that allow for a "private right of action". This gives individuals the right to sue spammers up to \$200 per message, up to a maximum of \$1 million. The potential here could be dramatic--individuals could join together for class-action suits to create a substantial settlement. The government can also pursue action against non-compliant senders, with a higher maximum fine of \$10 million.

Non-Email Messages To reiterate, the ECPA covers any "commercial electronic message" which is sent from, routed through, or accessed from Canada - not just email. This includes SMS, text messages, and more. It could also potentially apply to certain types of messages sent through social networking sites.

Bottom Line Use a clear and concise opt-in method, stating up front the purposes for which consent is being sought, the persons or entities seeking consent, and any other information about how information will be collected and used. Going one step further and using a confirmed or double opt-in process is even better. As mentioned above, most items are already covered in our BlueHornet Solution's standard procedures, but direct unsubscribe requests or complaints must be handled in a timely manner and if a consistent unsubscribe link is not used, these need to be kept active for at least 60 days if not indefinitely. Also, using third-party lists--where recipients did not grant their permission for you to send them email--has always been risky and against best practices, and now it is even more important to end their use. If you are concerned you may not have adequate consent from your recipients, feel free to get in touch with us info@infinitydirect.com.