
Faculty of Social Science

Faculty Publications

Canada's 'anti-spam' law comes into force on 1 July this year

Robin Bayley and Colin J. Bennett

June 2014

With permission from *Privacy Laws & Business*

https://www.privacylaws.com/Publications/int/PLB_International_Issues/PLB-International-Issue-129/

Citation for this paper:

With permission

Bennett, C. & Bayley, R. (2014). Canada's 'anti-spam' law comes into force on 1 July this year. *Privacy Laws & Business International Report*, 129, 19-20.

https://www.privacylaws.com/Publications/int/PLB_International_Issues/PLB-International-Issue-129/

Canada's 'anti-spam' law comes into force on 1 July this year

Organisations need to obtain prior consent for sending commercial emails or text messages in Canada. By **Robin Bayley** and **Colin Bennett**.

A new Canadian law regulates certain Internet activities that discourage commerce and is intended to deter spam (unwanted email solicitation) and other damaging and deceptive electronic threats such as identity theft, phishing and spyware.

The anti-spam provisions take effect on 1 July 2014. There are three general requirements for sending a commercial electronic message ("CEM" or an email or text message) to an electronic address under this legislation. Organizations subject to the law must obtain prior consent, provide identification information about the senders (including a postal address), and supply an easily effected unsubscribe mechanism.

Because its full name is approximately 53 words, it is referred to as "Canada's anti-spam law", or CASL. It also prohibits other practices such as unauthorized installation of spyware, malware and viruses (effective in 2015), email address harvesting, and misdirection or misrepresentation involving the use of any means of telecommunications.

The law applies to emails sent from or received in Canada, and not merely to such communications routed through Canada.

There are significant penalties for non-compliance, and officers and directors may be personally liable. Those illegally trafficking in personal information may also have to reimburse victims for costs. Administrative monetary penalties for CASL violations are up to CA\$1 million for individuals and CA\$10 million for businesses.

CONSENT

Under the CASL, organizations cannot readily rely on implied consent for sending emails. Before assuming consent, businesses should become familiar with the Enforcement Information Bulletins from the Canada Radio-Television and Telecommunications Commission

(CRTC), which provides examples of which practices do and do not meet the test. For instance, an opt-out process such as a pre-ticked box that the individual must click to "undo" is not compliant (bulletin 2012-549). Neither is a link to a privacy policy that informs users of secondary uses of their personal information, should they choose to do business with the organization. The consumer must have the option not to consent to secondary uses. An easy to understand overview of consent requirements from the government is found at: www.crtc.gc.ca/eng/casl-lcap.htm

IDENTIFICATION

Organizations and individuals must identify themselves and all the persons on whose behalf a commercial electronic message is sent. Hyperlinks may be used if it is not practical to list everyone on whose behalf messages are sent. Mere service providers involved in execution of the communication do not need to be listed. Identification requires a postal address.

The law prohibits posing as another organization, such as if an email re-directs an individual to another website than the user intends.

UNSUBSCRIBE

Unsubscribe options must be "readily performed" – that is, be simple, quick and easy for the end-user. The law allows a variety of means. Requests to unsubscribe must be acted on without delay and at no cost to the recipient. The CRTC enforcement bulletin 2012-548 provides further guidance. Many organizations already have effective and accessible unsubscribe options so this is not likely to be a major change.

ENFORCEMENT

The CASL amends three pieces of legislation, including the Personal Information Protection and Electronic Documents Act (PIPEDA), and gives

enforcement powers to the agencies that regulate those statutes. Three regulators share responsibility: the CRTC for administrative monetary penalties, the Competition Bureau for administrative monetary penalties or criminal sanctions under the Competition Act, and the Privacy Commissioner of Canada for violations of PIPEDA. The legislation also includes a private right of action and individuals or groups can bring private lawsuits, including class actions.

Violations and enforcement mechanisms are phased in over a three-year period. The Privacy Commissioner of Canada's powers are broadened to allow the Commissioner to share information with provincial and international counterparts in the context of investigations with inter-provincial or international implications. The Commissioner can now exercise discretion about whether to act or refer complaints.

The CRTC has the greatest role in enforcement. It will investigate transmission of unsolicited emails, and unauthorized installation of software and alteration of transmission data. An online spam reporting centre will be in place from 1 July on the CRTC website. Anyone will be able to report emails received without consent and emails with false or misleading content. The information gleaned will be available to all three regulators.

The Privacy Commissioner will concentrate on illicit personal information collection from unauthorized access to others' computers and email address harvesting from the Internet. The Competition Bureau will enforce scams and phishing using false or misleading representations and deceptive Internet marketing practices.

THE IMPACT ON INDUSTRY

As a result of a consultation process regarding spam that started in 2004, CASL contains many features desired

by legitimate businesses. The main impact for reputable businesses will be the anti-spam provisions. It will force a move from a norm of opt-out consent for marketing to that of opt-in.

Some critics are concerned about individual corporate officers being liable for fines and are worried that this will discourage individuals to volunteer for board membership. They also argue that the compliance cost to businesses and regulators will be high, and not lead to a noticeable decrease in spam and other prohibited practices. Some feel it will reduce Canadian competitiveness, as foreign firms will not be subject to such stringent regulation. Lawyers such as Maanit Zemel also report that CASL contains complex contradictory provisions, that it holds email service providers responsible for users' actions and that its application to social media is unclear. Supporters counter that all the other G-8 countries have such legislation already.

Organizations need to conduct reviews, and may need to change their consent practices for e-mail communication with current and prospective customers. There are also implications for database management, as new fields may be necessary to keep track of consent for different purposes. Information system reprogramming may be required to ensure that only email addresses associated with consent for a specific purpose are scooped up when compiling mailing lists. Further, existing agreements regarding the receipt of lists from other organizations may require amendment to take into account these new consent requirements.

Organizations are advised to audit the processes by which they compiled their current lists, and trace them back to the circumstances of their collection, through the organizations that supplied the addresses, right back to the individual to ensure consent. However, it may be more prudent for them to directly ask everyone on lists to consent to all the specific uses and disclosures that will be made of the email address and personal information associated with it. Opt-in rates can be higher with more granular choices. For instance, providing a yes/no choice for all potential and named uses is likely to yield lower

CONSENT FORM EXAMPLE: INSTITUTE FOR RESEARCH ON PUBLIC POLICY

Stay connected

Your consent is required

You currently receive e-mails from the **Institute for Research on Public Policy**, providing you with news about our publications and upcoming events. On July 1, 2014, Canada's new anti-spam law will come into effect and after this date, without your consent, we will not be allowed to send you this information.

To continue receiving updates please click on the **"I agree"** button below. You may withdraw your consent and unsubscribe from our e-mail list at any time.

Your privacy is important to us – [view our policy](#).

I agree

I disagree

consent rate than separating purposes and letting the consumer choose.

CONSUMER IMPACT

Leading experts such as Michael Geist, Canada Research Chair of Internet and E-commerce Law at the University of Ottawa, who participated in early consultation, have been critical of the ensuing law. Implementation delays allowed time for industry lobbying and numerous exceptions to the law's application were added. These include: business-to-business emails; for charities that send emails for fundraising purposes; for the first email sent as a result of a third party referral; for political parties and candidates; and for messages that respond to consumer complaints or inquiries.

Furthermore, Canadian regulators

are not expected to be able to effectively address spam and other prescribed practices originating from outside of Canada, especially where no similar laws exist, although they do have authority to work on joint enforcement with international authorities. Further, it is not yet clear how the spam reporting system will work and whether the CRTC will have the resources to deal with the volume of reports. Some of the most egregious unsolicited e-mail communications will, no doubt, continue to intrude and annoy.

Nevertheless, despite the obvious gaps and the problems with enforcement, the law is one of the strongest in the world. It is already prompting businesses to seek consent to the continued solicitations by email (see above). And consumers should get more control over the use of their personal information because consent for marketing will now be "opt-in", which has not hitherto been the norm.

TRANSPARENT LIVES

Professor Bennett is one of the editors and main authors of a recently published book on surveillance in Canada. 'Transparent Lives: Surveillance in Canada' details nine key trends in the processing of personal information, discusses how surveillance affects our lives and what could be done about it. The book is available free of charge at www.aupress.ca/books/120237/ebook/99_Z_Bennett_et_al_2014-Transparent_Lives.pdf

AUTHORS

Robin M. Bayley, Linden Consulting, Victoria BC, Canada, and Colin J. Bennett, University of Victoria, BC, Canada



27 YEARS
1987-2014

INTERNATIONAL REPORT

PRIVACY LAWS & BUSINESS

DATA PROTECTION & PRIVACY INFORMATION WORLDWIDE

'Right to be forgotten' ruling is an Internet privacy watershed

The right is to be limited only in certain cases where the public interest prevails. **Artemi Rallo** reports from Spain.

Contrary to most predictions, the decision of the Luxembourg-based European Union Court of Justice of 13 May 2014 (*Case C-131/12, Google vs AEPD*) resulted in the recognition of the 'right to be forgotten' online. The court has granted this right against Internet search engines in all circumstances, following the appeal by Spain's Data Protection Agency (AEPD). The resolution marks a watershed moment in the history of the Internet, given that its impact will affect both the fundamental rights of Internet users (particularly their privacy and the protection of their personal data) and the design of future Internet services (such as search

engines and social networks).

The European Court of Justice in the *Google vs AEPD* case has therefore demonstrated its commitment to personal data protection, both in its jurisdiction and in the constitutional and European legal framework. The court took as a starting point the high level appeal to protect personal data, considering Recital 10 of the EU Data Protection Directive 95/46. The court made a coherent interpretation of the directive, considering 'the protection of fundamental rights as a general principle of EU law', particularly given that the EU Charter of Fundamental Rights (CDFUE)

Continued on p.3

Search and access back issues by key words on PL&B's website

Subscribers can now conduct detailed research on data protection and privacy issues on the *Privacy Laws & Business* website and access:

- Back Issues since 2000
- Special Reports
- Materials from PL&B events
- Videos and audio recordings
- Search functionality giving you the most relevant content when you need it.

Further information at www.privacylaws.com/subscription_info
To check the type of subscription you currently have, contact glenn@privacylaws.com or telephone +44 (0)20 8868 9200.

Issue 129

June 2014

NEWS

2 - Comment

6 - DPAs' privacy enforcement sweep • Cloud accountability study

7 - Germany may see more direct action from consumer bodies

8 - EU makes limited progress with draft Data Protection Regulation

11 - Work progresses on Do-Not-Track • Snapchat settles with FTC • US Big Data group makes recommendations

18 - Canada and Malta appoint new commissioners • Australian Information Commissioner abolished

19 - Canada's 'anti-spam' law in force 1 July

24 - EU privacy seal on the cards

29 - CNIL to conduct 200 online inspections this year

31 - EDPS vacancy advertised again • Ireland's extensive audit programme

ANALYSIS

12 - APEC's CBPRs: Two years on – take-up and credibility issues

16 - South African law imposes strict cross-border transfer rules

30 - Big Data and the competitive advantage of privacy

LEGISLATION & REGULATION

9 - Brazil adopts Marco Civil Internet law

21 - India's draft The Right to Privacy Bill 2014 – will the BJP enact it?

MANAGEMENT

5 - Hard times for companies operating in Germany

27 - Belgium's DPA makes pragmatic Recommendation on cookies

PL&B Services: Publications • Conferences
Consulting • Recruitment • Training • Compliance Audits
Privacy Officers Networks • Roundtables • Research

**Electronic Versions
of PL&B Reports
are Web-enabled**

Allows you to click from web addresses to websites

INTERNATIONAL
report

ISSUE NO 129

JUNE 2014

PUBLISHER**Stewart H Dresner**
stewart.dresner@privacylaws.com**EDITOR****Laura Linkomies**
laura.linkomies@privacylaws.com**ASIA-PACIFIC EDITOR****Professor Graham Greenleaf**
graham@austlii.edu.au**SUB EDITOR****Tom Cooper****REPORT SUBSCRIPTIONS****Glenn Daif-Burns**
glenn.daif-burns@privacylaws.com**CONTRIBUTORS****Artemi Rallo**
Universitat Jaume I, Spain**Nigel Waters**
Pacific Privacy Consulting, Australia**Nerushka Deosaran**
Norton Rose Fulbright, South Africa & Australia**Robin M. Bayley**
Linden Consulting, Canada**Colin J. Bennett**
University of Victoria, BC, Canada**Catherine Erkelens**
Bird & Bird, Belgium**C  drine Morli  re**
Bird & Bird, Belgium**Eduardo Ustaran**
Hogan Lovells International, UK**Julia de Oliveira**
PL&B Correspondent**PUBLISHED BY**Privacy Laws & Business, 2nd Floor,
Monument House, 215 Marsh Road, Pinner,
Middlesex HA5 5NE, United Kingdom**Tel: +44 (0)20 8868 9200****Fax: +44 (0)20 8868 5215****Email: info@privacylaws.com****Website: www.privacylaws.com****Subscriptions:** The *Privacy Laws & Business* International Report is produced six times a year and is available on an annual subscription basis only. Subscription details are at the back of this report.

Whilst every care is taken to provide accurate information, the publishers cannot accept liability for errors or omissions or for any advice given.

Design by ProCreative +44 (0)845 3003753
Printed by Rapidity Communications Ltd +44 (0)20 7689 8686

ISSN 2046-844X

Copyright: No part of this publication in whole or in part may be reproduced or transmitted in any form without the prior written permission of the publisher.

   2014 Privacy Laws & Business

“ ” **comment**

EU tightens the net on non-EU based companies

At *PL&B*, we cherish the close relationships we have formed over the years with Data Protection Authorities globally. This issue includes an article by Professor Artemi Rallo, former Director of Spain's Data Protection Agency, on the recent Google and 'Right to be Forgotten' decision (p.1). In April, we benefited from the expertise of German Lander DPAs in our two-day seminar, the highlights of which you can read on pp.5-7.

International transfers continue to be a burning issue. The EU has made some progress on this front – Binding Corporate Rules and the US Safe Harbor are likely to be two important instruments (see p.8), and the Justice ministers also agree that EU rules should apply to foreign companies if they do business in the EU. India is discussing a draft law that would leave outsourcing outside the scope of the law. For Indians, however, the law would provide comprehensive protection (p.21). In South Africa, the data transfer rules are strict – read an analysis on p.16. Will APEC and Cross Border Privacy Rules provide a solution for APEC member states? No, says our Asia-Pacific Editor (p.12).

In Belgium, the DPA has issued cookie guidelines for consultation (p.27), and in Canada, the new Privacy Commissioner is partially responsible for the enforcement of the new anti-spam act (pp.18, 19) that establishes similar protections to those already available in the EU. In Brazil, the ground-breaking new Internet law divides opinion as it creates obligations for foreign companies (p.9). In the EU, the debate around Big Data continues (p.30), and the draft Regulation may bring about a privacy seal (p.24).

Latin American developments, the EU draft regulation, international transfers and privacy seals are among topics that will be discussed at *New Horizons ~ New Risks*, our 27th Annual International Conference in Cambridge, 30 June to 2 July, at Queens' College.

We invite you to join us for the privacy event of the year! To register, go to www.privacylaws.com/annualconference

Laura Linkomies, Editor

PRIVACY LAWS & BUSINESS

Contribute to PL&B reports

Do you have a case study or opinion you wish us to publish? Contributions to this publication and books for review are always welcome. If you wish to offer reports or news items, please contact Laura Linkomies on Tel: +44 (0)20 8868 9200 or email laura.linkomies@privacylaws.com.

Your Subscription includes

1. Six Reports a year

The *Privacy Laws & Business (PL&B) International* Report, published since 1987, provides you with a comprehensive information service on data protection and privacy issues. We bring you the latest privacy news from more than 100 countries – new laws, bills, amendments, codes and how they work in practice.

2. Online search function

Subscribers can search the *PL&B* website to access: back issues since 1998; special reports, slides, videos and recordings from *PL&B* events.

3. Regular e-news

Subscribers receive updates about relevant news as and when it happens. Choose international and/or United Kingdom data protection news.

4. Helpline Enquiry Service

Subscribers can request information about the current status of legislation and other information.

5. Index

Search a country, subject and company index (1987-2014)
[www.privacylaws.com/
Publications/report_index/](http://www.privacylaws.com/Publications/report_index/)

Electronic Option

The electronic PDF format enables you to: receive the Report on publication; click-through from email and web addresses; and follow links from the contents page to articles.

Subscription Discounts

Discounts for 2-4 users or 5-25 users and 2 years (10%) or 3 years (15%). See www.privacylaws.com/subscribe

Privacy Laws & Business has clients in more than 50 countries, including 25 of the Global Top 50, 24 of Europe's Top 50, 25 of the UK's Top 50 in the Financial Times lists.

Privacy Laws & Business also publishes the United Kingdom Report, a publication which ranges beyond the Data Protection Act to include the Freedom of Information Act and related aspects of other laws.

Subscription Form

Subscription Packages

(VAT will be added to PDF subscriptions within the UK)

Single User Access

- PL&B International* Report Subscription **£500**
 UK/International Reports Combined Subscription **£800**

Subscription Discounts

Discounts for 2-4 users or 5-25 users
Number of years: 2 (10% discount) or 3 (15%)

Go to www.privacylaws.com/subscribe

Special academic rate – 50% discount on above prices – contact the *PL&B* office

Subscription Includes:

Six new issues of each report, on-line access to back issues, special reports, and event documentation.

Data Protection Notice: *Privacy Laws & Business* will not pass on your details to third parties. We would like to occasionally send you information on data protection law services. Please indicate if you do not wish to be contacted by: Post email Telephone

Name:

Position:

Organisation:

Address:

Postcode: Country:

Tel:

Email:

Signature:

Date:

Payment Options

Accounts Address (if different):

Postcode:

VAT Number:

- Purchase Order
 Cheque payable to: *Privacy Laws & Business*
 Bank transfer direct to our account:
Privacy Laws & Business, Barclays Bank PLC,
355 Station Road, Harrow, Middlesex, HA1 2AN, UK.
Bank sort code: 20-37-16 Account No.: 20240664
IBAN: GB92 BARC 2037 1620 2406 64 SWIFTBIC: BARCGB22
Please send a copy of the transfer order with this form.

American Express MasterCard Visa

Card Name:

Credit Card Number:

Expiry Date:

Signature:

Date:

Please return completed form to:
Subscriptions Dept, Privacy Laws & Business,
2nd Floor, Monument House, 215 Marsh Road,
Pinner, Middlesex HA5 5NE, UK
Tel +44 20 8868 9200 Fax: +44 20 8868 5215
e-mail: sales@privacylaws.com

20/06

www.privacylaws.com

Guarantee

If you are dissatisfied with the *Report* in any way, the unexpired portion of your subscription will be repaid.