

CASL

CANADA'S ANTI-SPAM LEGISLATION

SURVIVAL GUIDE



A Quick Summary

Canada's Anti-Spam Legislation (CASL) – one of the most aggressive anti-spam laws in the world - will take effect in July 2014.

It has been a long journey for this piece of legislation that began its story in May 2004 with the [Federal Task Force on Spam](#). Over the years, the Government of Canada has received input from hundreds of stakeholders with an interest in responsible electronic messaging, in an effort to create what it hopes is a comprehensive law.

The final regulations for CASL were released Dec. 4, 2013, which provided strict guidelines on what is, and is not, acceptable. In addition, it included important exceptions for charities, third-party referrals, and political parties, along with other key modifications.

Unrestricted implied consent will become a thing of the past. So if you're emailing or texting people in Canada, you'd better make sure you have their express permission to do so (or valid implied consent), because the consequences could be very expensive.

Compliance planning should go into high gear now and many organizations are unsure of how to prepare. We set up this survival guide to provide you with the essential information to navigate the path ahead.

This free guide outlines in layman's terms: the regulations, timing, requirements, penalties and exemptions surrounding CASL. Consent is at the heart of the new law. The guide helps organizations identify whether or not they have proper consent, and if not, how to secure it prior to the imminent deadline, via a step-by-step action plan.

Guide Map

Overview of CASL	5
What is CASL Trying to Achieve?	6
CASL Timeline	6
Phased Implementation	7
Transitional Period for Implied Consent	7
Full Legal Text	8
Final Regulations (and Recent Modifications)	9
CASL's Bite	11
Penalties for Violating CASL	12
Who Does This Law Affect?	12
How is CASL Enforced?	12
CASL Requirements	13
Main Requirements of CASL	14
Exemptions From CASL	14
Differences Between CASL and Can-Spam Act	16
In-Depth Look at CASL Consent	17
Express Consent	18
Implied Consent	19
How To Prepare for CASL	21
Step 1: Know The Date	22
Step 2: Get Out That Rage	22
Step 3: Internal Awareness	22
Step 4: Identify Key Players in Your Organization	23
Step 5: Initial General Assessment	23
Step 6: Deep Dive Into Existing Databases	24
Step 7: Customers with Implied Consent	25
Step 8: Start Emailing Your Implied Consent Contacts Before July 2014	25
Step 9: Whip Every Inbound Data Process Into Shape	26
Step 10: Ready. Set. Re-Confirm!	26

Step 11: Purge Non-Compliant Subscribers Before CASL Goes Live	28
Step 12: CASL is Here!	28
Step 13: Document Your Efforts	29
Step 14: No Deceptive Messages Going Forward	29
Step 15: Keep an Eye on Things	29

Will CASL Ultimately Be a Good Thing? 30

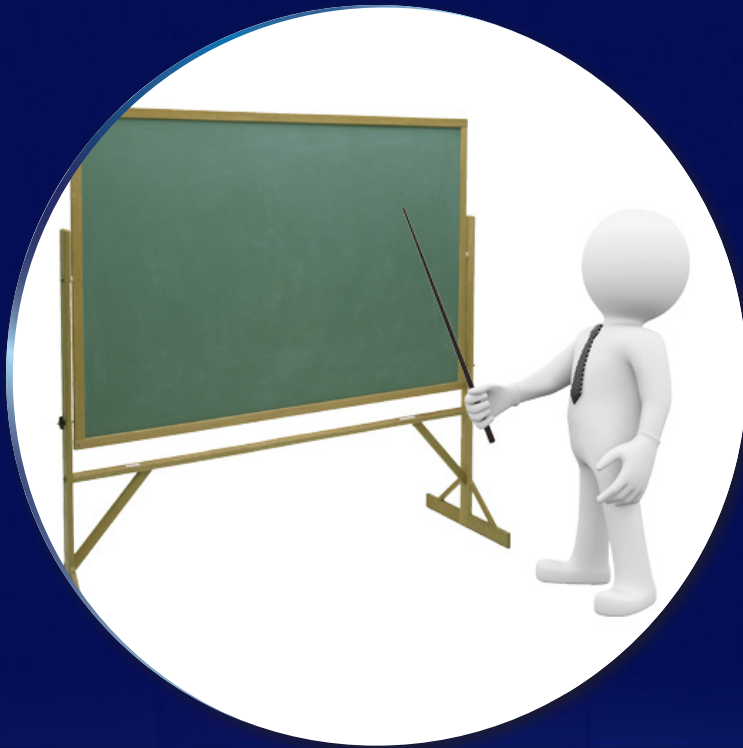
Thoughts on “No”	31
Thoughts on “Yes”	32

CASL Survival Guide Online Version:
<http://www.eliteemail.com/learning-center/casl/>

Legal Disclaimer

This guide is intended to provide our general comments on the new law. It is not intended to be a comprehensive review nor is it intended to provide legal advice. Readers should not act on information in the publication without first seeking specific advice from their lawyer.

OVERVIEW OF CASL



What is CASL Trying to Achieve?

The official stated goal of Canada's Anti-Spam Legislation (CASL) is "An Act to promote the efficiency and adaptability of the Canadian economy by regulating certain activities that discourage reliance on electronic means of carrying out commercial activities."

When you translate that to the real world, it essentially means that the government is trying to stop the sending of [spam](#) to Canadians by imposing a new set of strict rules that govern all commercial electronic messages (CEMs).

While the objective of protecting Canadians from spam (i.e. [identity theft](#), [phishing](#), [spreading spyware](#), etc.) is a noble one that most people can support, the new regulations have a broader view of electronic communication, and therefore broader implications. So even if your organization has been following email best practices for years, the new rule book still changes the game.

For the remainder of this guide we will simply use the term "email" or "SMS/text" to mean CEM, unless indicated otherwise.

CASL Timeline

The legal evolution of CASL has played out as follows:

May 25, 2010	Bill C-28 First Reading
Dec. 15, 2010	Royal Assent (Passed)
July 2011	Regulations Drafted
July 2011	Regulations "Gazetted" For Review
Sept. 7, 2011	Draft Regulations Comment Deadline
Mar. 2012	CRTC Regulations Gazetted
Jan. 5, 2013	Industry Canada Draft Regulations Published For Comment
Dec. 4, 2013	Industry Canada Final Regulations
July 1, 2014	CASL Takes Effect
Jan. 15, 2015	CASL Computer Program Provisions Takes Effect
July 1, 2017	CASL Private Rights of Action Takes Effect

Phased Implementation

While most aspects of the law come into effect in July 2014, some components will be phased in.

Unsolicited installation of computer programs and software – January 15, 2015

The deadline for unsolicited installation of computer programs and software is January 15, 2015. Most other countries in the world don't address this.

Private right of action – July 1, 2017

The right of action, which would allow consumers and businesses to take civil action against anyone who violates CASL, will be deferred for three years. This gives breathing room to businesses and helps the Canadian courts avoid a potential glut of litigation for an initial period while the new law is put into practice.

Transitional Period for Implied Consent

Section 66 of CASL creates a special transitional period for scenarios where there is implied consent based on an existing business or non-business relationship. According to the CRTC's FAQ:

Section 66 deems implied consent for a period of 36 months (unless the recipient withdraws consent earlier) where there is an existing business or non-business relationship and the relationship includes the communication of CEMs. During the transitional period, the definition of existing business or non-business relationship is not subject to the limitation periods (6 months and 2 years) that would otherwise be applicable under CASL, for implied consent to exist.

The issue of implied and express consent is discussed later in this guide. The reason this transitional period is noteworthy is because typically there is a two year window after a customer makes a purchase (or six months after they submit an inquiry) where you have 'implied' consent to communicate with them.

However, with this transitional period, anyone you have implied consent from prior to CASL taking effect (July 1, 2014), will actually extend to 36 months (instead of the six post inquiry or 24 months post purchase). As long as you've already been communicating with them.

That being said, the definitions of "business" and "non-business relationship" can become murky, so the best and safest course of action is to get express consent even during this transitional window.

Full Legal Text

You can read the full law here:

<http://laws-lois.justice.gc.ca/eng/acts/E-1.6/index.html>

The Regulatory Impact Analysis Statement from Industry Canada helps to qualify some of the components of the law and can be seen here:

<http://fightspam.gc.ca/eic/site/030.nsf/eng/00271.html>

The main Government of Canada website related to CASL can be accessed here:

<http://fightspam.gc.ca/>

FINAL REGULATIONS (AND RECENT MODIFICATIONS)



A few key modifications were included in the publication of CASL's final regulations that were greeted as good news by the marketing industry.

You now do not have to re-qualify existing express consents in your database

The former draft regulation stipulated that even if you had express consent under Canada's privacy law, you had to go out and get fresh consent. Under express consent, the intended recipient gives explicit permission (electronically, in writing, or orally with documentation) to a business or charity to send emails. According to John Gustavson, President/CEO of the Canadian Marketing Association (CMA), this "was going to be an enormous cost for big business."

The good news is that under the final CASL regulations an organization does not have to requalify or reconfirm contacts that have already given that organization express consent. This is important because it means express consent obtained before CASL goes live, will be recognized as being compliant after CASL is live.

However, it's important to note that certain scenarios of "implied consent" will not be recognized. Under the Personal Information Protection and Electronic Documents Act (PIPEDA) if a person does not clearly decline consent (such as in opt-out options and boxes), consent is granted. This is no longer the case under CASL and any mailing list subscribers falling under this umbrella would need to be reconfirmed.

Private Right of Action has been deferred

As described in the previous section the right to private action, which would allow consumers and businesses to take civil action against anyone who violates CASL, will be deferred until July 2017.

For the time being the government will be the only entity to prosecute transgressors of the new law. But the pressure is still on for companies to comply by July 2014. The government has indicated it will "go after bad actors first — the real spammers, the really egregious ones". Legitimate businesses that are trying to comply should have some time to get onside.

CASL will not apply to messages sent to people in countries listed as having their own anti-spam legislation

There was previously some concern about Canadians sending emails to another country where there was a different set of spam laws. The recent changes amend this to get rid of the "double jeopardy" scenario as you don't have to follow both (sets of regulations); you only follow where the recipient is.

Fundraising is now exempt

Registered Canadian charities and political parties do not have to worry about CASL for fundraising efforts. They do still have to comply with unsubscribe requests. It should also be noted that American political parties and charities are not exempt like their Canadian counterparts.

CASL's BITE



Penalties for Violating CASL:

CASL has sharp teeth; penalties for violations can range from up to \$1 million for individuals and \$10 million for companies.

Who does this law affect?

The law is not limited to just Canadians; it takes effect any time a Canadian computer is used to access the email (any commercial electronic message). So, if you're in the U.S. or overseas, but your email newsletter also goes to recipients in Canada, then all these rules apply.

According to one CRTC official "If the spammer is offshore, we have the ability under the law to cooperate with foreign governments, to share information and to bring proceedings together against individuals that are offshore." While the likelihood of the CRTC seeing through offshore proceedings is questionable, the risk is real for those overseas who flout CASL's rules.

How is CASL Enforced?

There are three government agencies tasked with enforcing CASL: Competition Bureau of Canada, Office of the Privacy Commissioner of Canada, & Canadian Radio-television and Telecommunications Commission (CRTC).

CASL REQUIREMENTS



Main Requirements of CASL:

Although CASL's roots might have been as a weapon against spam, its resulting implications extend to all businesses, even those who have been abiding by common best practices. Here are some of the key highlights of CASL:

- Multiple rules about consent. A key focus of CASL is detailing the exact ways you can acquire consent to send emails. Moreover, it makes consent an absolute requirement in most scenarios.
- Requests for consent must also include a statement that the person can withdraw their consent at any time.
- When obtaining consent, it must be an affirmative action. This means you cannot pre-check form fields to obtain legitimate consent.
- Your message must have a working unsubscribe mechanism. If someone requests to be unsubscribed it must be processed within 10 days.
- Unsubscribes cannot be reconfirmed. So, there is no sending of "Are you sure you want to unsubscribe?" e-mails.
- No misleading or false subject lines or sender names. You must make it very clear who you are when collecting data and when sending messages.
- Must include a physical postal mailing address and one additional way to contact the sender (e.g. web form, email address or phone number). PO boxes are accepted as a valid address.
- When sending on behalf of another organization, that organization must be identified.
- If you send an initial email to someone based on a referral, the person who made the referral must be stated in the message.

The implications for companies is that significant changes will need to be made to their existing databases as well as the procedures (both online and offline) for when data is added to mailing lists.

Exemptions From CASL

While most organizations will be impacted by CASL in some form, there is a detailed list of items that are exempt from CASL's reach.

One primary complaint about CASL is that the regulations are so broad that it requires a long list of exemptions. This opens up the criticism that it is impossible to imagine every specific scenario that warrants an exemption to ensure it is included. Nonetheless, it does make these

exemptions an important part of the law.

The following scenarios are exempt from CASL's consent and form/unsubscribe requirements:

- Messages sent by an individual to an individual recipient with whom the sender has a personal or family relationship. (Industry Canada has specific definitions for each type of relationship.)
- Messages sent to a person that relates directly to an inquiry for commercial goods and services.
- Interactive two-way voice communications (e.g. telemarketing), faxed or messages sent by phone.
- Messages sent by an employee, representative, consultant or franchisee of an organization to another employee, representative, consultant or franchisee of the same organization (i.e. internal communications) which concern the activities of the organization.
- Messages sent by an employee, representative, consultant or franchisee of an organization to an employee, representative, consultant or franchisee of another organization (i.e. business-to-business communication), as long as the organizations have a relationship and the message concerns the activities of the organization to which the message is sent.
- Messages sent in response to an individual's request, inquiry or where the message was solicited by the person receiving the message. This is largely the "email reply" exemption.
- Messages sent in regards to a legal obligation or to enforce or provide notice of existing/pending legal rights or actions.
- Messages sent and received on a social media platform, if the information and unsubscribe function are readily available on the user interface through which the message is accessed. In addition, the person who was sent the message consents to receive it either expressly or by implication.
- Messages sent by a person who reasonably believes the message will be accessed in a foreign country that is on the list of accepted countries that maintain their own anti-spam laws. ([view country list](#))
- Messages sent by or on behalf of a Canadian registered charity (as defined in the Income Tax Act), assuming the message is primarily about raising funds for the charity. Note that these organizations in other countries (i.e. U.S.A.) are not exempt. It is also important to highlight that it is only registered charities, so other organizations that conduct fundraising initiatives that might even issue donation receipts are not included in this exemption.
- Messages sent by or on behalf of a Canadian political party or organization, or a person who is a candidate for publicly elected office, assuming the message has the primary

purpose of soliciting a contribution as defined in the Canada Elections Act. Note that these organizations in other countries (i.e. U.S.A.) are not exempt.

Differences Between CASL and Can-Spam Act

CASL isn't just an "email" law (similar to the American [CAN-SPAM Act of 2003](#)), it covers other digital channels such as text messages (SMS) and installed computer programs. That means becoming CASL-compliant isn't an exercise focused exclusively on email mailing lists, but other databases as well.

While the Can-Spam Act is based on an opt-out model, CASL is on the complete opposite side and based on the opt-in model. This means that under CASL, emails can only be sent when the recipient, through implied or express consent, requests the email, whereas under Can-Spam the messages can be sent until the recipient requests they stop.

One other difference is that CAN-SPAM only applies if the email has a primary intent that is commercial. CASL applies if there is any commercial activity encouraged. A good example of this is a transactional message that follows a customer purchase. A business may send them an email that summarized their recent transaction along with a secondary marketing message, such as other products they may be interested in. CASL would apply to this message because there is some commercial activity encouraged, where CAN-SPAM would probably not apply since it's not the primary reason for the email.

IN-DEPTH LOOK AT CASL CONSENT



The underlying key to CASL is consent. You just cannot do anything without consent. If you walk away with one key theme from this guide, let it be consent, consent, consent!

CASL essentially outlines two primary types of consent: Express Consent & Implied Consent.

Express Consent

Express consent, sometimes referred to as explicit consent, is basically the most obvious type of consent where the recipient has given you direct permission to email them. This type of consent is far less ambiguous than implied consent because the permission is clearly captured without much concern for legal interpretation.

There are still some requirements to ensure that express consent is valid including:

- Clearly describe the purposes for requesting consent.
- Provide the name of the organization/person seeking consent, and identify on whose behalf consent is sought, if different.
- Provide contact information such as a mailing address (PO boxes are valid), telephone number, email address or website address.
- Indicate that the recipient can unsubscribe or withdraw consent at any time.

One important thing to note is that express consent must be an affirmative action. This means you cannot have a pre-checked box on a registration form to secure consent.

The two most common ways that express consent is acquired are:

1. A mailing list sign up form on your website.
2. A confirmation link in an email.

Whenever you obtain express consent, it is important that you document everything. As the sender it is your responsibility to prove that you received proper express consent. This means tracking items like the date, time, IP address, form used, link clicked in email, etc.

It is also worth knowing that express consent does not expire until the recipient revokes it.

Implied Consent

Implied consent is the more ambiguous side of the consent game because it can be a bit more subjective on whether or not it exists in a specific scenario.

This type of consent is essentially the one where you can email someone because you have an existing relationship with them, even though they never explicitly requested that you email them.

According to CASL, consent will be implied in the following scenarios:

- The recipient and sender have an “existing business relationship” or an “existing non-business relationship.” This is elaborated further below.
- If the recipient has “conspicuously published” their email address, the publication is not accompanied by a statement that the recipient does not wish to receive unsolicited messages, and the message is relevant to the person’s business, role, functions or duties.
- If the recipient has disclosed their email address to the sender without indicating that they do not want to receive unsolicited messages and the message is relevant to the person’s business, role, functions or duties. This can be thought of as the “business card” consent.

The topic of an existing business or non-business relationship needs to be elaborated further as this will often be a key area of discussion when trying to figure out if implied consent exists.

An “existing business relationship” exists where the sender and recipient have engaged in business together within the previous two years from the date the message is sent.

This could mean that the recipient purchased a product/service from you or entered into a written contract.

One important thing to note is that during the two year window, if they make another purchase from you, the clock resets to another two years. That being said, it is often a good idea to secure express consent at some point during the two years (usually right away) so that you never have to worry about the implied consent expiring.

Another form of “existing business relationship” exists when the recipient has made an inquiry to the sender in the previous six months. This is the method of consent that lets you respond to new customer emails without having to worry about violating CASL. Once again, it is good practice to try to secure express consent from these people so you can email them past the six month window.

An “existing non-business relationship” is defined as a relationship that exists from the recipient’s activities as a donor or volunteer for a registered charity, political party or political candidate, a member of a club, association or voluntary organization. It is important to note that this is very narrow in scope and not necessarily what you would assume.

If educational institutions, medical providers, hospitals, charities, clubs, and other non-business organizations provide services to the public they cannot automatically claim that an existing non-business relationship exists. There was thought that the final regulation would adjust this, but it did not happen. So, unless the non-business relationship fits into the really tightly defined definition (i.e. donor to a charity), then you would need a business relationship or express consent.

REMINDER:

CASL has a special transitional period so that the two year and six month windows discussed above are extended to 36 months from the date CASL takes effect, provided that you have emailed the contact previously.

HOW TO PREPARE FOR CASL



*CASL is coming! CASL is coming!
What should you do?
Don't panic, calm down. Take a deep breath.*

This guide will walk you through all the important steps to get you from where you are today all the way through to the magical land of CASL compliance.

Step 1: Know The Date

Go into every calendar you look at, whether it's your Outlook calendar, Gmail calendar, or that good ol' paper calendar on your bulletin board and put a note for July 1, 2014 with CASL in big bold letters.

Everything you do from this point forward is to get ahead of the July deadline so that once CASL goes live, your organization is in good shape.

While there is a transition period that applies in certain scenarios, you don't really want to have a game plan based on special exceptions, your goal is to be fully compliant.

Step 2: Get Out That Rage

If you're like most marketing folks, shortly after circling July 1 on your calendar, you are going to be pretty mad about all the new work you have to do related to CASL and you'll probably be fairly angry at those lawmakers in Ottawa.

Get that all out of your system. Take a few minutes to bang your desk, raise your fists in the air, shout out some curse words, and any other action that you should probably do with your office door closed.

You don't want to be harboring this rage going forward since you want to be focused on what you have to do, not being mad that you have to do it.

Step 3: Internal Awareness

At this point, you've read this entire guide so you are equipped with an abundance of CASL knowledge. But, most people in your organization probably don't have a clue about this game-changing legislation. Now is the time to fix that.

Bring everyone in the organization, from senior management all the way down, up to speed on what's happening. You don't have to get into the nitty-gritty details, but you do want to put this on everyone's radar so they are not completely caught off guard later when you start talking about changes, revised workflows, etc.

Step 4: Identify Key Players in Your Organization

CASL has very broad rules that can impact many parts of your organization and all of them need a detailed review.

Take a moment and figure out whom in your company is involved in some way with something that would be affected by CASL.

If you're a small company, then it may just be you, but in a bigger company, this could involve people in marketing, sales, HR, etc.

The benefit to building your team of internal CASL compliance superheroes is that you can be much more confident that nothing will get overlooked or slip through the cracks. You don't want to risk making your marketing department compliant, while completely ignoring all the emails the sales department is sending.

Step 5: Initial General Assessment

Pull out the fine-toothed comb because it's now time to look at every aspect of your organization to pinpoint the areas where CASL can have an impact.

The key things you want to identify are:

- Online data capture (e.g. mailing list signup forms, landing page forms, lead generation forms, etc.)
- Offline data capture (e.g. trade shows, phone leads, received business cards, etc.)
- Offline forms (e.g. registration forms, etc.)
- Existing mailing lists
- CRM (customer) databases
- Current triggered emails (e.g. welcome email, confirmation email)
- Current email campaigns (including engagement metrics)
- Current manually sent emails

The list of items you identify here will ultimately form key things on your to-do list.

Step 6: Deep Dive Into Existing Databases

It's now time to take a good long look at all of our existing databases.

If you've been following email marketing best practices, you may have a large contingent of subscribers that have already given you express consent as defined by CASL. Industry Canada has clearly stated that express consent that is compliant with PIPEDA will also be compliant with CASL. The interpretation of this is still a bit murky, so if you want to be extra cautious you can treat everyone on your database like they have not given you express consent.

But, if you want to try to shuffle some people into the "express consent" group, here is an example of what a typical Elite Email customer would look for:

- You have put a mailing list sign up form on your website.
- The form is clear that people are signing up to receive emails from you and it clearly identifies that your organization is going to be the sender.
- The form in no way tricks people to join your mailing list by having a sneaky pre-checked checkbox that opts them in.
- Upon form submission a welcome email is sent to the supplied address.
- The welcome email contains a confirmation link (for double opt-in) that the new subscriber must click.
- Throughout this process, your email marketing system has captured the date/time of the new sign up, along with the subscriber's IP address.
- At no point did this subscriber unsubscribe (automatically by clicking a link or by emailing you) or request to be removed from your database.

If at this point, you feel you have concrete evidence that a subscriber explicitly requested your emails, then you can treat those people as CASL-compliant.

Create a new segment of your mailing list for these subscribers and make sure they are removed from the "everyone else" group of addresses that are not compliant.

You now have a nicely defined database of those addresses that will require further confirmation. You'll come back and use this data again very soon, but let's keep heading down the 'getting organized' path first.

Step 7: Customers with Implied Consent

In Step 6 your goal was to find people who had given you express consent. Now in Step 7 it's time to look for implied consent. Realistically, you want to get express consent from everyone, but identifying implied consent is important because it means you can continue emailing them even while you work towards getting express consent.

Plus, with CASL's special transitional period, you can have three full years before the implied consent expires. That's a very long time and isn't something you want to miss out on!

Hopefully you have a CRM system that tracks the date of a customer's last purchase (or contract). This is very important because CASL builds a window of implied consent based on that date. If you're not tracking last purchase date, then put a new item on your to-do list: "Track last purchase date".

The other item you have to determine is whether or not emails are currently being sent to these customers. The transitional period only applies if messages are being sent before CASL comes into effect, otherwise it's the normal two-year rule. We tackle this in Step 8 to give you an extra edge!

Coming out of this step, your goal is to have a clear picture of which customers qualify as having implied consent. These are the folks you can keep emailing even if you don't have express consent.

Step 8: Start Emailing Your Implied Consent Contacts Before July 2014

Ready to get a little crafty?

The CASL transition rule that gives you three years for implied consent instead of the typical two years is only valid if you've been emailing those contacts before CASL goes live.

So, find everyone in Step 7 who you identified as having implied consent but who you are not currently emailing. Then, go over to your marketing people and tell them that you absolutely need to find something (...something of value!) to email these people. The objective is to get the messages flowing now, so you can secure an extra year to get express consent.

Keep in mind, the focus here is not on going back to every customer you've ever had since you really do not want to bother people that you know truly don't care to hear from you. But rather to find the customers you've gotten in the "not too distant past" and start communicating with them.

Once you've got those emails going, your CASL timeline now extends further for these contacts, because it's three years from July 2014.

Step 9: Whip Every Inbound Data Process Into Shape

In Step 5 you did a high level summary of all the areas of your organization that feed in data both online and offline. Now it's time to make sure every one of those processes follows the new CASL rules.

If you go back in this guide to the section about "Express Consent", it will show you a clear checklist of items you must have in order for express consent to be valid. Be meticulous because once you come out of Step 9, every new subscriber you get should be CASL-compliant.

This is also the step where you're going to want to get everyone you identified in Step 4 so that you can double check (...and triple check) that every process has been thoroughly audited. Leave no stone unturned!

Take a good long look at every sign up form you have online and make sure you don't have any pre-checked boxes because that is often a common mistake. Also, look at messages that trigger after the form is submitted (such as a welcome email) to make sure the content lends itself to full compliance.

For processes that happen orally, this is a lot trickier because you have less of a paper trail. If you're capturing email addresses over the phone, it is generally a good idea to send those subscribers a welcome email right away because then you can capture their click on a confirmation link and that acts as your evidence of express consent. If you're recording and archiving every call, then having a well-crafted express consent script that the subscriber agrees to will also be valid, but then you have to store and catalog a whole lot of recordings. Before moving on, take a moment and grab a screenshot of all your online forms. This way you can do one final check that you've hit every item on the requirements list and also so you have further evidence of the exact form people would have filled out.

Step 10: Ready. Set. Reconfirm!

This is a very important step because if done effectively, it will salvage the majority of your mailing lists even once CASL is in full force.

In Step 6 you identified those subscribers that have already given you express consent and those that haven't. Right now you're going to focus on those that haven't in an effort to get them shifted over to the other column.

The goal is to send these subscribers an email and get them to click a link that confirms they wish to continue receiving your emails. When they click this link, the date, time and IP address must be tracked, as that becomes your hard evidence for express consent.

Keep in mind, opening your emails or clicking on other links does not qualify as express consent. The subscribers needs to click a link that clearly identifies that they are very clearly requesting to receive your emails.

Looking at some example link text:

“Visit Our Website” == Not even close to express consent

“Click here to confirm your interest in receiving our emails” == BINGO!

There are two core types of reconfirmation messages:

- Dedicated Confirmation Campaigns
- Embedded Requests in Typical Campaigns

Dedicated Confirmation Campaigns

This is a campaign where the sole focus is on acquiring confirmation. The email should be very clean and simple with a clear call to action of clicking the confirmation link. There should be very little competing content, which can act as a distraction from clicking that ever-important confirmation link.

While these campaigns can be very effective, you don't want to overuse them because there's very little intrinsic value from the subscriber's point of view. One of the reasons they'll want to continue receiving your emails is because they are of value to them (ie. discounts, information, news, etc.), and yet in an ironic twist, this specific confirmation email doesn't add all that much value to their day.

If you continually try to hammer these confirmation campaigns at your subscribers, they may not only choose not to confirm, but they may unsubscribe even sooner.

This type of mailing should be treated as a tool in your arsenal, but not one that should be abused.

Embedded Requests in Typical Campaigns

This is a campaign where you are sending out your usual content, but within that message you have an additional call to action for confirmation.

The reason this type of campaign works is because you have time before CASL takes effect to still email everyone on your database without worrying about specific CASL compliance. The goal is to seize the opportunity on every email to move people from lacking express consent to having express consent.

The advantage with these embedded requests is that your email still has the same value it always does in the eyes of your subscriber. You're not pestering them with a message in their inbox that exclusively asks them to click the confirmation link. This means you don't have to schedule extra campaigns on your content calendar because every planned campaign between now and July 2014 is acting as a confirmation email as well.

The disadvantage is that since your email is filled with a lot of competing content and calls to action, it makes it more difficult to get the subscriber to click the link you want.

In terms of strategy, a mix of both dedicated confirmation emails and embedded requests works best. You don't have to just choose one or the other. Take a look at your planned campaigns and map out when you want to send your dedicated confirmation emails. Also, keep track of the frequency at which you are asking people to reconfirm. While that reconfirmation is important to you, it's also important you don't frustrate your subscribers.

Remember, from this point forward a key success metric of each campaign is how many confirmations you secured. Don't neglect your other engagement metrics, but add this one into the mix.

CASL is coming, there is no longer any doubt. With only four months left (from the time of publication of this guide) before the law comes into affect, businesses should start preparing now.

Step 11: Purge Non-Compliant Subscribers Before CASL Goes Live

If you've always wanted to be a doctor, now would be the time to say "scalpel please" because you're about to slice and dice your way through your organization's databases.

Anyone who has not yet given you express consent and does not meet the criteria for implied consent needs to go.

While this may make you sad, and you should pause to shed a tear, you need to remember that it is for the greater good. Plus, after all your efforts to reconfirm these contacts, if they still didn't express interest, then there's a good chance these were not your high value subscribers anyway.

Once you're done with this step, all of your organizations databases should only have people that are CASL-compliant and all new data coming in is going through a process that will satisfy CASL. In short, this is a milestone moment.

Step 12: CASL is Here!

The date you've had circled on your calendar for so long has arrived.

Pat yourself on the back for doing a great job with all the preparation. Let your boss know you deserve a raise... or at least a trophy of some kind because this wasn't easy.

Also, equally as important is calling all your other marketing friends who are in a panic and rub it in their face that your organization is sitting pretty. (Just don't tell them the folks at Elite Email told you to do that!)

Step 13: Document Your Efforts

Take a little bit of time and document everything you have done to become compliant.

If you get into trouble with CASL, but can demonstrate that you made very strong efforts (due diligence) to comply with all the rules and have done everything to obtain proper consent, then that will play a factor in the event a lawsuit comes up.

It's for this reason that it's important to track and document everything so you can cover yourself later with a stronger case if things get messy.

This might also be a good time to take a look at your organization's privacy policy to see if it needs updating.

Step 14: No Deceptive Messages Going Forward

At this point, your organization is in great shape on the consent side of things, but CASL also has rules to prevent sending deceptive messages.

Make sure the people who are responsible for crafting your organization's email campaigns know that there's a new rulebook to follow which really frowns upon shady activity that tricks people.

Step 15: Keep an Eye on Things

Getting CASL-compliant is one thing, but staying CASL-compliant is another.

You worked hard to get your organization to this point. You definitely don't want someone to do something that makes things fall out of compliance.

People in your organization may try to work around your new policies, but don't let them. Be strict! If they question why you are being so strict, remind them of the million dollar fines that exist for violating CASL. They probably don't want to cover those fines for your organization, so they'll probably understand why you want to strictly play by the rules.

WILL CASL ULTIMATELY BE A GOOD THING?



There are many articles that discuss whether CASL is good or bad for Canada. That discussion on either side of the argument could span for pages and pages. While the goal of this guide is not to go incredibly in-depth into these arguments, it is important to touch on them briefly so that you can carry on a conversation at the water cooler.

Thoughts on “No”

CASL will not stop spam. Canadians will have as much spam in their inbox after July 1, 2014 as they did before. The most egregious spammers were not following the rules before and they’re not going to follow them now. Plus, most of the spam that Canadians receive originates from outside the country despite the claim that international offenders will be prosecuted, which is easier said than done.

Spamhaus, a highly respected anti-spam organization, publishes a list of the [Top 10 worst countries that send spam](#). This list generally includes USA, China, Russia, Ukraine, Japan, United Kingdom, Brazil, France, India and Germany.

Who is noticeably absent from that list of countries? Canada! The country that now has the most strict spam law in the entire world, isn’t even on the list of countries that really need a strict spam law.

So, if the law is not going to impact the actual bad spammers, who does it effect? The answer: legitimate businesses that were probably employing “best practices” beforehand. But now those businesses have the burden of having to comply with an unbelievably broad regulation that governs all forms of electronic communication.

There are a lot of people in the country who strongly believe that the costs and annoyance for companies significantly outweigh the purported benefits, particularly in the case of smaller companies.

Plus, the ISPs of the world and all of the anti-spam software companies have gotten really good at weeding out the good emails from the bad. By that token, Canadian inboxes were in a large sense already protected from spam, so did we really need this massive piece of legislation?

The law has also been criticized as overkill with the size of the fines not matching the crime (one million dollar individual fine and ten million dollar corporate fine) and is out of proportion for the nuisance of spam.

Think about the small business who certainly doesn’t have a lawyer on retainer to help navigate the murky waters of CASL. A salesperson working for that business sends an email to a potential customer in an effort to drum up a new account. That email is not CASL-compliant, but was sent with the best of intentions and is far from flagrant spam. When the recipient gets that email, and assuming it is after July 1, 2017, when the “private right of action” kicks in, that recipient can sue the small business for ten million dollars. That one email has the potential to cause a sequence of events that puts that company out of business

because it definitely cannot afford a penalty like that. So, how is this law benefiting the Canadian economy, which is fueled by small businesses that find themselves in a similar position?

The law is also written in a way where it can be so complicated to interpret that the only true winners of this legislation are the lawyers who are going to be paid tremendous amounts of money to decipher what is or is not compliant.

While the goal of CASL may have been a noble one to help Canadians, it has manifested itself into a piece of legislation that will hinder commerce in Canada and put Canadian organizations of all sizes at a disadvantage against their international counterparts.

Thoughts on “Yes”

The world has gone digital, but Canada does not have a comprehensive rulebook that establishes what is and is not allowed. Without rules, there is anarchy that can spiral out of control, and a modern day economy cannot thrive with that sort of wild west mentality. CASL corrects that problem by prescribing a set of practices and procedures that sets everything on the right track for future prosperity.

From a consumer perspective, it should cut down on a lot of unwanted emails, allowing Canadians to be more productive. This is not to say that it will stop all spam, but at the very least Canadian organizations will no longer be able to secretly add you to their mailing list.

If an organization has been following good practices, including a proper double opt-in procedure (also called “closed loop”), having a valid unsubscribe link, not being deceptive at all, then that organization is largely compliant already.

The grunts and groans of organizations that have to make changes are because their hand is being forced to make a change from what they are currently doing to following a more stringent set of best practices enforced by law. Setting guidelines that explicitly describe how to obtain consent, instead of leaving it completely arbitrary, will aid consumers and businesses.

The goal of CASL is not to force everyone to slash the size of their mailing list, but rather take some time to look inwards and see if the organization is actually emailing the right people. The special “transition” period gives organizations extra time to continue emailing people that have implied consent, so there is no major disruption due to the law taking effect. For those that don’t have implied consent, running a reconfirmation campaign will let an organization identify who is actually interested in their message so they can be focused on. After all, sending an email to 1,000 people that are highly interested in your content is much better than sending an email to 10,000 people that won’t even open up your email.

Furthermore, there stands to be a big benefit for those organizations that do everything properly and become CASL-compliant simply because there will be less clutter in a subscriber’s inbox. In a pre-CASL era, a consumer may receive emails from ten different

organizations, where each one is competing for attention in the inbox. In a post-CASL era, that same consumer is only going to get emails from three different organizations that they really care about. If your organization is one of those, then you can expect more focus and greater engagement.



Call Us

Toll Free 877-789-ELITE (3548)

Canadian 416-747-6111

American 212-845-9894

Email Us

Sales sales@eliteemail.com

Support support@eliteemail.com

Media media@eliteemail.com

5511 Steeles Ave. W, Suite 200
Toronto, Ontario, M9L 1S7

Follow Us



<https://twitter.com/eliteemail>



<https://www.youtube.com/eliteemailvideos>



<https://www.facebook.com/eliteemail>



<http://blog.eliteemail.com/>



<https://plus.google.com/+EliteEmail>



<http://www.linkedin.com/company/elite-email>

Visit us Online

<http://www.eliteemail.com/>

CASL Survival Guide Online Edition

<http://www.eliteemail.com/learning-center/casl/>

CASL SURVIVAL GUIDE
BY EliteEmail