

Privacy & CASL

Deborah Evans

May 2017

Agenda

Today's Goals

- Privacy
 - ✓ Privacy in Canada
 - ✓ Privacy at Rogers
 - ✓ 10 Principles of PIPEDA
 - ✓ The Reasonable Person Test
 - ✓ Consent
 - ✓ Data - Personal Information
 - ✓ Reporting
 - ✓ Data Across Borders
 - ✓ Retention & Access
- CASL
 - Legislation
 - What is it?
 - Defining CEMs
 - Expiring Consent

PRIVACY

Today's Goals

By the end of today's session, you will:

Understand the 10 Principles of PIPEDA

Understand How To Be CASL Compliant

Understand the CRTC Rules For Confidentiality

Become an advocate for privacy by promoting best practices.

Who Is Watching Big Brother?

- Do you know the various laws that govern privacy in Canada?
- What makes a company like Rogers different from Google when it comes to privacy?



Rogers is committed to ensuring that our customers' personal information is safe and secure and we consider protection of our customers' privacy one of our highest priorities. Rogers has long-established processes to fulfill our obligations as a good corporate citizen to follow the law and contribute to public safety. We take these matters very seriously.

Understanding Privacy In Canada

There are a number of laws in Canada that relate to privacy rights, and there are various government organizations and agencies responsible for overseeing compliance with these laws.

The key factors that determine what laws apply and who oversees them include:

- The nature of the organization responsible for the personal information
- Is the organization a federal government institution subject to the Privacy Act?
- Is it a provincial or territorial government institution?
- Is it a private-sector organization?
- Is it engaged in commercial activities?
- Is it a federal work, undertaking or business (FWUB)?
- The location of the organization (where is it based?)
- The type of information (is it personal information, and if so, what type of personal information is it. i.e., is it health information?)



Public, Private & Provincial Legislation

The Privacy Commissioner of Canada (PCC) oversees both the federal Privacy Act and PIPEDA. The PCC may audit the privacy practices of organizations suspected of a breach of PIPEDA, and may receive and investigate complaints of non-compliance. Provincial privacy laws are enforced by provincial Information and Privacy Commissioners (IPCs) or Ombudsmen, who can investigate complaints and issue binding orders requiring compliance. In addition, individuals have a private right of action for privacy breaches in Québec, B.C., Alberta and Ontario

PROVINCIAL

Every province and territory has its own public-sector legislation and the relevant provincial act will apply to provincial government agencies, not the Privacy Act.

FEDERAL

Canada has two federal privacy laws, the Privacy Act, which covers the personal information-handling practices of federal government departments and agencies, and the Personal Information Protection and Electronic Documents Act (PIPEDA), the federal private-sector privacy law.

PRIVATE

Canadian businesses are subject to federal or provincial privacy protection legislation governing both customer and (with some exceptions) employee information. The federal Personal Information Protection and Electronic Documents Act (PIPEDA) applies to all private sector organizations in Canada, except in provinces that have enacted “substantially similar” legislation. PIPEDA also applies when personal information is disclosed across a provincial border in the course of commercial activity and in most situations where an organization in Canada receives or transmits personal information from or to a destination outside Canada.

PUBLIC

Public sector privacy laws apply in the federal and most provincial and municipal jurisdictions. Similar to the U.S. federal Privacy Act, the federal Privacy Act and provincial counterparts require government departments, agencies, most Crown corporations and municipal government bodies to define, and notify individuals of, the lawful, authorized purposes for their collection of an individual’s personal information and to provide access to personal information they hold that is requested by individuals.

Privacy Compliance

Rogers' privacy practices are in accordance with all federal and provincial laws and regulations. We are compliant with the Personal Information Protection and Electronic Documents Act (PIPEDA) and where applicable with the privacy rules established by the Canadian Radio-television and Telecommunications Commission (CRTC).

The Office of the Privacy Commissioner of Canada oversees compliance with PIPEDA. PIPEDA generally applies to:

- Private-sector organizations carrying on business in Canada in the provinces or territories of Manitoba, New Brunswick, Newfoundland and Labrador, Northwest Territories, Nova Scotia, Nunavut, Ontario, Prince Edward Island, Saskatchewan, or Yukon but not their handling of employee information.
- Private-sector organizations carrying on business in Canada when the personal information they collect, use or disclose crosses provincial or national borders but not their handling of employee information.
- Federally-regulated organizations carrying on commercial activity in Canada, such as a bank, airline, telephone or broadcasting company, etc., including their handling of health information and employee information.

The Office of the Privacy Commissioner of Canada investigates complaints about the misuse of personal information.

- *Personal Information Protection and Electronic Documents Act (OPC)*
 - ✓ Consent: implied vs express
 - ✓ Sharing of Personal Information
 - ✓ Use / disclosure / transfer of Personal Information
 - ✓ Monetization of Personal Information – OBA
 - ✓ Privacy Breaches – current (voluntary) vs future (mandatory)

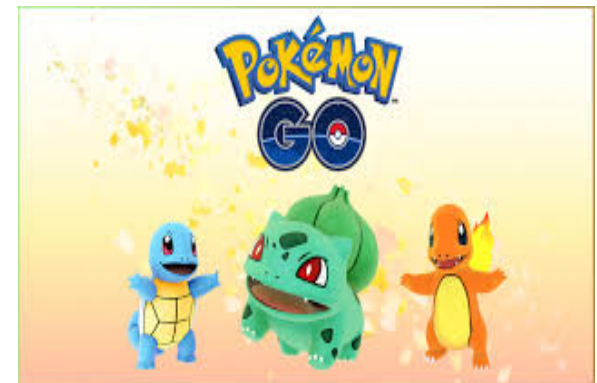
Enforcement = Damage to Company Reputation

Do You Ever Think About Privacy Settings In the Real World?

Think about the things you do daily....

Record the following on a flipchart :

1. Have you ever read a privacy policy before agreeing to a service, contract or product?
2. Think of 3 forms of technology you use daily:
 - i. Do you know what information they collect about you?
 - ii. Do you know how this information is used?



10 Principles of PIPEDA

Rogers' privacy practices are in accordance with all federal and provincial laws and regulations. We are compliant with the Personal Information Protection and Electronic Documents Act (PIPEDA) and where applicable with the privacy rules established by the Canadian Radio-television and Telecommunications Commission (CRTC)

1	Be Accountable	<ul style="list-style-type: none">• Comply with all 10 of the principles of Schedule 1.• Appoint an individual (or individuals) to be responsible for your organization's compliance.• Protect all personal information held by your organization or transferred to a third party for processing.• Develop and implement personal information policies and practices
2	Identify the Purpose	<ul style="list-style-type: none">• Before or when any personal information is collected, identify why it is needed and how it will be used.• Document why the information is collected.• Inform the individual from whom the information is collected why it is needed.• Identify any new purpose for the information and obtain the individual's consent before using it.
3	Obtain Informed Consent	<ul style="list-style-type: none">• Specify what personal information you are collecting and why in a way that your customers and clients can clearly understand.• Inform the individual in a meaningful way of the purposes for the collection, use or disclosure of personal data.• Obtain the individual's consent before or at the time of collection, as well as when a new use of their personal information is identified.
4	Limit Collection	<ul style="list-style-type: none">• Do not collect personal information indiscriminately.• Do not deceive or mislead individuals about the reasons for collecting personal information.

10 Principles of PIPEDA Continued

5	Limit Use, Disclosure and Retention	<ul style="list-style-type: none">• Use or disclose personal information only for the purpose for which it was collected, unless the individual consents, or the use or disclosure is authorized by the Act.• Keep personal information only as long as necessary to satisfy the purposes.• Put guidelines and procedures in place for retaining and destroying personal information.• Keep personal information used to make a decision about a person for a reasonable time period. This should allow the person to obtain the information after the decision and pursue redress.• Destroy, erase or render anonymous information that is no longer required for an identified purpose or a legal requirement.
6	Be Accurate	<ul style="list-style-type: none">• Minimize the possibility of using incorrect information when making a decision about the individual or when disclosing information to third parties.
7	Use Appropriate Safeguards	<ul style="list-style-type: none">• Protect personal information against loss or theft.• Safeguard the information from unauthorized access, disclosure, copying, use or modification.• Protect personal information regardless of the format in which it is held. <p><i>Note: PIPEDA does not specify particular security safeguards that must be used. Rather, the onus is on organizations to ensure that personal information is adequately protected.</i></p>
8	Be Open	<ul style="list-style-type: none">• Inform customers, clients and employees that you have policies and practices for the management of personal information.• Make these policies and practices understandable and easily available.

10 Principles of PIPEDA Continued

9	Give Individuals Access	<ul style="list-style-type: none">• When requested, inform individuals if you have any personal information about them.• Explain how it is or has been used and provide a list of any organizations to which it has been disclosed.• Give individuals access to their information.• Correct or amend any personal information if its accuracy and completeness is challenged and found to be deficient.• Provide a copy of the information requested, or reasons for not providing access, subject to exceptions set out in Section 9 of the Act.• An organization should note any disagreement on the file and advise third parties where appropriate.
10	Provide Recourse	<ul style="list-style-type: none">• Develop simple and easily accessible complaint procedures.• Inform complainants of their avenues of recourse. These include your organization's own complaint procedures, those of industry associations, regulatory bodies and the Office of the Privacy Commissioner of Canada.• Investigate all complaints received.• Take appropriate measures to correct information handling practices and policies.

10 Principles – Open Discussion

Let's discuss...

Who is accountable for privacy at Rogers?

Where can we access information on Rogers privacy practices?



How long is personal information retained?

What are 2 reasons Rogers collects personal information?

The Reasonable Person Test

Privacy is always reviewed in the context of the “reasonable person”. Although companies have the ability to identify any uses they believe are acceptable within their privacy policy, this will always be evaluated against what the “reasonable person” and their expectations.

NECESSITY

Is the measure demonstrably necessary to meet a specific need?

- What specific problem they hope to solve, and whether the proposed system is essential for satisfying the need.

EFFECTIVENESS

Is it likely to be effective in meeting that need?

- It's important to remember that even low failure rates can have a significant impact when a system is scaled up to involve thousands or even millions of people.

PROPORTIONALITY

Would the loss of privacy be proportionate to the benefit gained?

- In testing for proportionality, organizations should bear in mind that certain actions are more privacy-sensitive than others. The more sensitive the information the result should promise extraordinary benefits.

ALTERNATIVES

Is there a less privacy-invasive way of achieving the same end?

- Is the proposed solution in the best interest of Canadians?

Consent

The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate. The form of the consent sought by the organization may vary, depending upon the circumstances and the type of information. In determining the form of consent to use, organizations shall take into account the sensitivity of the information. In obtaining consent, the reasonable expectations of the individual are also relevant.

What is Implied Consent?

There are a few forms of implied consent, including:

- **Conspicuous publication:** The information is published in plain sight, for example, on a website or in a trade magazine.
- **Disclosure:** The information is given to you, for example, people give you their business card or address.
- If people conspicuously publish their address or give it to you, then you have implied consent to send them messages **related to their work**. These are valuable forms of implied consent for business-to-business marketing since they allow cold calling, but only if the address was acquired legitimately and the message is relevant to the recipient.
- **Existing business relationship:** The person has made a transaction, an inquiry, an application or a written contract for the purchase or barter of products, goods or services.
- **Existing non-business relationship:** The person is a member of your organization or has provided volunteer work, a donation or a gift.

What is Express Consent

Express consent is very specific

- **Express consent** means that a person has clearly agreed (orally or in writing) to receive a commercial electronic message. It is not time-limited, unless the recipient withdraws his or her consent.

How Does Rogers Obtain Consent?

We may obtain implied or express consent to the collection, use, and disclosure of information in one of the following ways:

- **In writing; or**
- **by electronic confirmation via the internet; or**
- **verbally, where an audio recording of the consent is retained by us; or**
- **through other methods, as long as a record of the consent is created by the customer, by us, or by a third party acting on Rogers' behalf.**

Example: An individual buying a subscription to a magazine should reasonably expect that the organization, in addition to using the individual's name and address for mailing and billing purposes, would also contact the person to solicit the renewal of the subscription. In this case, the organization can assume that the individual's request constitutes consent for specific purposes. On the other hand, an individual would not reasonably expect that personal information given to a health-care professional would be given to a company selling health-care products, unless consent were obtained. Consent shall not be obtained through deception.

Case Study - Bell Relevant Advertising Program (RAP)



Background

- In August 2013 Bell announced its “Relevant Advertising Program” (RAP), which would use customer network data (i.e. internet, telephone, and television network use) and account/ demographic information (including full postal code, gender, age range, credit rating, and payment history) to serve Bell customers with targeted ads.
- Bell was not obtaining customer consent to include them in the RAP. Customers could opt-out or receiving the ads, however, Bell would continue to “track” the customer and augment their profile in case the customer opted back in to the program in the future.
- The Office of the Privacy Commissioner of Canada (OPC) received an unprecedented number of public complaints, leading to an comprehensive privacy investigation of the RAP.

OPC Findings

The OPC investigation determined that Bell was not obtaining adequate customer consent for the RAP, and that the customer’s express opt-in is required for this type of program based on the following:

1. Use of sensitive information
 - Bell is using sensitive URLs for the purpose of generating customer profiles.
 - Compiling internet, telephone and television network use accompanied with account/demographic information made it more sensitive.
2. Reasonable expectations of Bell’s customers
 - Bell was using information it had for the purposes of delivering its primary services (i.e. telecom) for the new secondary purpose (i.e. targeted ads).
 - Bell delivers paid services, for which customers may pay up to hundreds of dollars per month;
 - Bell is using the information it has to enable the delivery of third-party ads; and
 - Bell is a trusted agent provided sensitive personal information by their customers in order to gain access to mobile, internet, telephone and television communications in Canada.

PI| PII| Publically Available

Personal Information (PI)

- Information related to an individual i.e. name, address, phone number.

Personally Identifiable Information (PII)

- Personal information that can identify a specific individual

Publicly available information under PIPEDA - for collection without knowledge and consent of the individual

- Name, address and telephone number of a subscriber that appears in a telephone directory that is available to the public, where the subscriber can refuse to have the personal information appear in the directory.
- Name, title, address and telephone number of an individual that appears in a professional or business directory, listing or notice, that is available to the public, where the collection, use and disclosure of the personal information relates directly to the purpose for which the information appears in the directory, listing or notice.
- Personal information in a registry collected under a statutory authority and there is a right of public access by law; collection, use and disclosure of the personal information must relate directly to the purpose for which the information appears in the registry.
- Personal information that in a record or document of a judicial or quasi-judicial body, that is available to the public; collection, use and disclosure must relate directly to the purpose for which the information appears in the record or document.
- Personal information in a publication (e.g. magazine, newspaper) where the individual has provided the information.

Can the business use information from web browsing history, Facebook etc. to build my user profile?

Big Data – Open Discussion

Let's discuss...

Is it reasonable to use my internet history to market products and services to me?.... Google does it

Is using my TV viewing history to help me pick my cable package convenient or concerning?



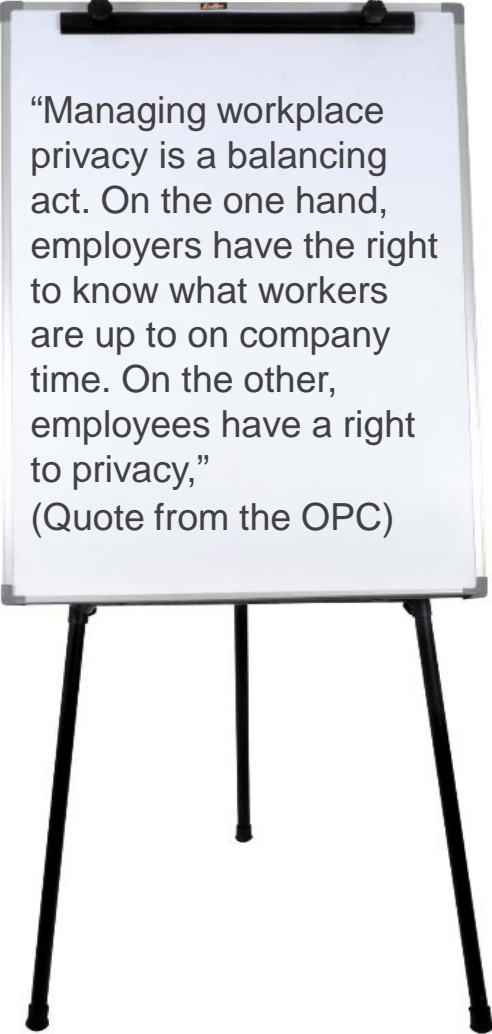
What is the difference between personal information and aggregated information?

Can companies collect information from my social media account for data analytics?

GPS In the Workforce

What does the OPC Say?

- Using GPS to dispatch vehicles is likely to lead to better service for the company's customers and also could help locate missing vehicles.
- While using GPS to track a vehicle is not overly privacy invasive, routinely evaluating worker performance based on assumptions drawn from GPS information impinges on individual privacy.
- The use of GPS as an employee surveillance tool may be acceptable in certain situations, which are defined and communicated to employees beforehand. However, a company should not routinely use GPS to monitor its workforce.
- Clearly explain to employees how GPS would be used to check up on them, and also develop a policy outlining an appropriate process of warnings and progressive monitoring.
 - Train managers about the appropriate use of the technology.



“Managing workplace privacy is a balancing act. On the one hand, employers have the right to know what workers are up to on company time. On the other, employees have a right to privacy,”
(Quote from the OPC)

Transparency Reporting

Who Has Accessed My Information?

As part of our privacy commitment to our customers, Rogers has taken an active lead by publishing an annual Transparency Report for the last three years.

The report provides details about the requests for information about our customers that we receive from government and law enforcement agencies.

Rogers has taken active steps to safeguard our customers' information and defend their privacy rights. For example, following a Supreme Court ruling, we now require a court order or warrant (or equivalent) to process customer name and address checks and child sexual exploitation assistance requests, unless there is an immediate risk as outlined in the Criminal Code.



Breach Reporting



Currently the Office of the Privacy Commissioner (OPC) does not require mandatory reporting. Mandatory data breach notification requirements in PIPEDA will come into force once the Government passes regulations intended to provide greater clarity and specificity of the rules. New rules (TBD 2017) will require organizations to notify the Office of the Privacy Commissioner of Canada (OPC) and affected individuals if personal information is lost or stolen and there is a risk of harm as a result.

VOLUNTARY REPORTING

- The CPO/ Associate CPO will review privacy incidents to determine if we should report to the OPC
- Voluntary reporting requires that we provide:
 - Location, date of incident and discovery
 - Description of incident
 - Cause (if known)
 - Estimated number of individuals affected
 - Type of individuals effected (e.g. customers, employees)
 - Type of personal information involved
 - Brief description of action taken to contain breach
 - Has anyone been notified of incident (e.g. affected individuals, law enforcement, other) and when (date)?

Are you storing
my information
in another
country?

There is nothing in PIPEDA that prevents organizations from outsourcing the processing of data (unless detailed in a contract i.e. Government contracts). However, regardless of where information is being processed—whether in Canada or in a foreign country—organizations subject to PIPEDA must take all reasonable steps to protect that information from unauthorized uses and disclosures while it is in the hands of the third-party processor.

- Organizations must also be satisfied that the third party has policies and processes in place, including training for its staff and effective security measures, to ensure that the information in its care is properly safeguarded at all times.
- Organizations need to make it plain to individuals that their information may be processed in a foreign country and that it may be accessible to law enforcement and national security authorities of that jurisdiction. They must do this in clear and understandable language. Ideally they should do it at the time the information is collected. Once an informed individual has chosen to do business with a particular company, they do not have an additional right to refuse to have their information transferred.
 - Terms of service: Personal information collected in connection with the provision of the Services may be stored and processed in or outside Canada and may be subject to the laws of other jurisdictions.
- When personal information is in the hands of a third-party service provider operating on foreign soil, it is subject to the laws of that country and no contract can override that. This could mean, for instance, that the organization may be obliged to respond to a subpoena or other mechanism that would give law enforcement officials access to personal information.

Retention & Access

Account holders have the right to access personal information gathered by Rogers/Fido upon request. We have established processes in place for customers to request this information outlined in the Privacy Policy and Nova Doc POL38

RETENTION

Rogers will only retain your account or personal information for as long as necessary to fulfill the purpose we collected the information, or for sufficient time to allow you access to the information if it was used to make a decision about you or your account. Once we no longer require your account or personal information it will be destroyed or de-identified

ACCESS REQUESTS

Rogers ensures that customer information is accurate, complete and up-to-date. Customers can ask to review that information and have the opportunity to challenge its accuracy and completeness and request amendments, as appropriate, by contacting our Chief Privacy Officer.

Access & Retention – Open Discussion

Let's discuss...

How long is my information retained?

Do you have copies of my text messages?



What is Rogers doing to support privacy and lawful access?

*Stingrays...
What's up with that?*

CASL

Telemarketing and Anti-Spam

The CRTC has established rules for both unsolicited telemarketing and sending Commercial Electronic Messages

- Unsolicited Telemarketing Rules (CRTC)
 - ✓ Do Not Call: Internal and National
 - ✓ Automated Dialing Assistance Devices (ADADs)
- Canada's Anti-Spam Legislation (CRTC)
 - ✓ Commercial Electronic Messages vs service message – consents & unsubscribe
- Both set of rules recognize existing business relationships

Enforcement = Fines + Jail Time

Why should we care about CASL?

What is CASL?

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, and to amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act

Canada's Anti-Spam Legislation (CASL)

- CASL came into effect July 1, 2014, and established the framework for what businesses can do when using electronic channels to promote or market themselves or their products and services to an electronic address of Canadians (for example via email or text message).
- The law applies to both Canadian and non-Canadian businesses.
- Effective January 15, 2015, CASL's rules about installing computer programs came into effect, making it illegal to install programs on devices such as computers, mobile phones, or tablets without the owner's consent.

Rogers has a duty to understand and comply with the law.

Rogers must establish an internal compliance regime to ensure that everyone sending commercial messages understands and complies with the law.

Are You Sending a CEM?



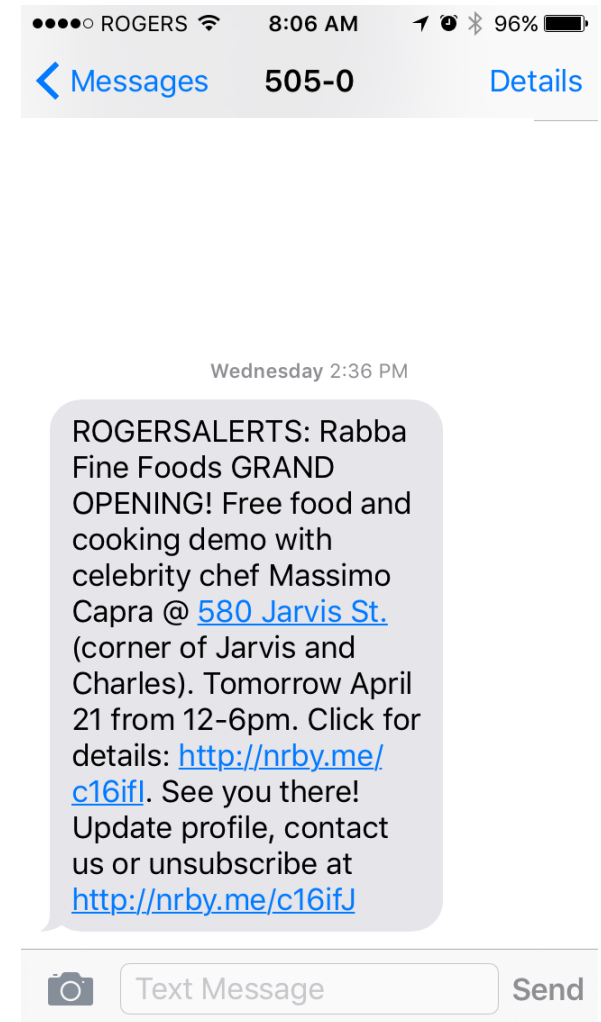
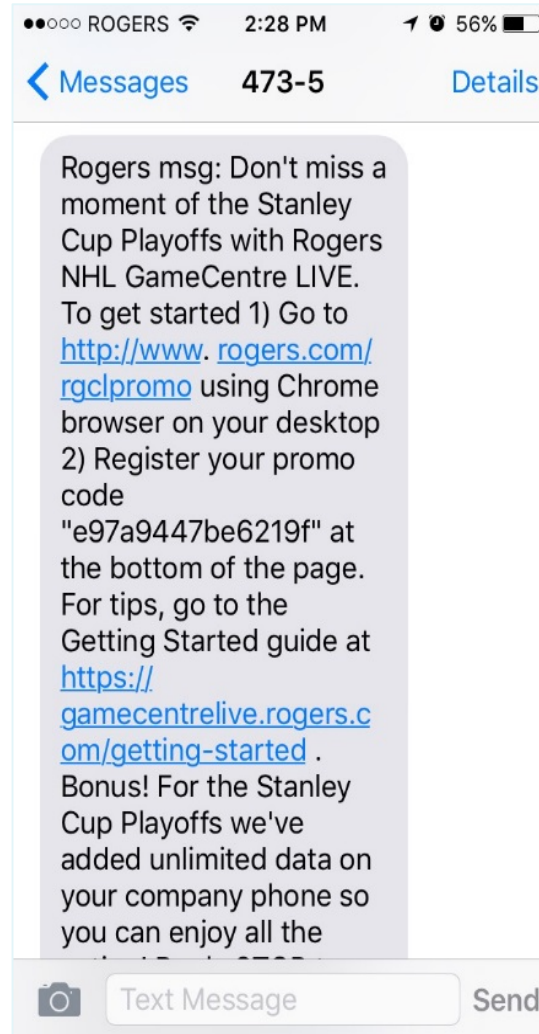
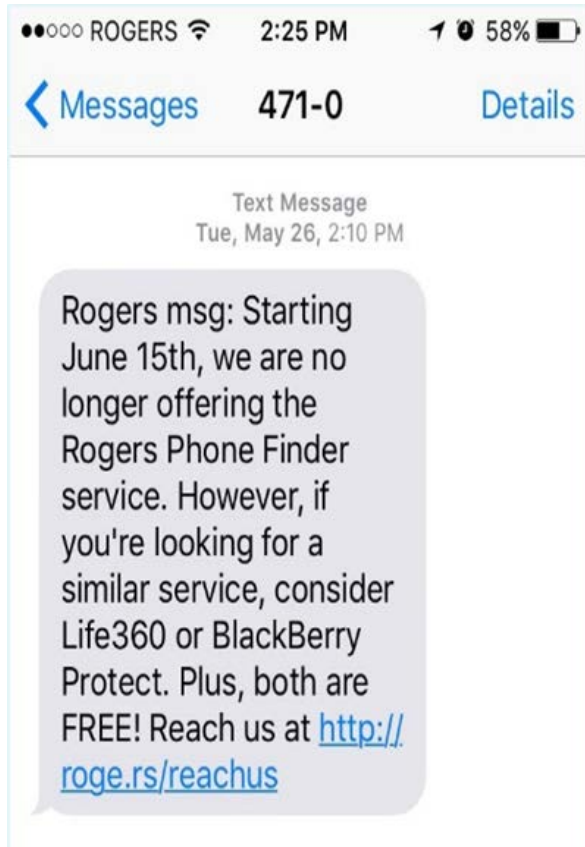
How to identify if an electronic message is a Commercial Electronic Message or CEM?

- Is the message being sent to an electronic address such as an email, text, or direct message on social media?
- Is one of the purposes of the message to encourage participation in a commercial activity, such as making a purchase, upgrading a service, or renewing a service agreement. Or does it promote Rogers or one of your companies, affiliates, or services?
- Is there a hyperlink in the message that direct the customer to a page where the primary purpose is to sell a product or service. (e.g. data day passes)?

The message is not a CEM if it does not contain any promotional content, responds to an inquiry or must be sent by regulation or legal authority.


Every CEM MUST include details on how to unsubscribe

How Well Can You Identify a CEM?



How Well Can You Identify a CEM?

You've almost completed your Rent-to-Own rental period.
Can't see this email? [View online](#)



ROGERS.

We've got good news!

Dear DUNCAN,

You have almost completed your Rent-to-Own rental period, which means you will soon own your NextBox™.

You will see a one-time \$1 Rent-to-Own purchase option charge (plus tax) on one of your next two bills for each NextBox with a completed Rent-to-Own rental period. As soon as that bill is paid, you'll own those NextBox (es) and no more rental fees will apply. No further action is required on your part.

Continue to enjoy your favourite shows, movies and sports on your NextBox and keep an eye out for upcoming NextBox enhancements.


Call 1 888 ROGERS1 if you have any questions

© 1995-2015 Rogers Communications

[Contact Us](#) | [Unsubscribe](#) | [Privacy Policy](#) | [rogers.com](#)

Rogers Communications | One Mount Pleasant Road | Toronto ON M4Y 2Y5

Can't see this email? [View online](#)



ROGERS.

Enjoy all the latest movies and TV shows during this festive season.

Rogers Anytime TV™ | Rogers On Demand™ | iWatch™

Action/Adventure

LEGENDS OF TOMORROW
Series Premiere
Jan 21 at 5:30pm ET

TRACERS
Available On Demand Jan 23

COLONY

SICARIO

Wild Things with Dominic Monaghan
Season Premiere
Jan 5 at 9pm ET

DITRET
Available as of January 26


Use your remote or
CALL 1 888 ROGERS1 TO UPGRADE YOUR TV PACKAGE
Not seeing what you like?
Update your preferences [here](#) >

Check your programming guide for exact times.

© 1995-2015 Rogers Communications

[Contact Us](#) | [Unsubscribe](#) | [Privacy Policy](#) | [rogers.com](#)
Rogers Communications | One Mount Pleasant Road | Toronto ON M4Y 2Y5
[\(+1\) SEE FULL DETAILS](#)

View your Rogers bill 2015



ROGERS.

Your online bill is ready.

You have 18,218 Rogers Plus Rewards points as of this month's bill.

We just want to say thanks for choosing online billing and let you know that your Rogers bill is ready. Simply sign in to your MyRogers™ account online or view it now on the mobile app.

Here are your billing details:

Account number: 524569670
Current bill total: \$1,000,000.00
Thank you for pre-authorizing your payment. We'll withdraw this amount from your account on or after Nov 27, 2015.

[View bill](#)

Need help understanding your bill? No problem! Find the answers you're looking for [fast](#).

Do more from your MyRogers™ account
You can do much more than just view your bill, you can also:

- View your voice, text and data usage
- Pay your bill
- Check your account balance
- Update your account information
- View bill details

[Learn more](#) about MyRogers™

© 1995-2015 Rogers Communications

[Contact Us](#) | [Unsubscribe](#) | [Privacy Policy](#) | [rogers.com](#)
Rogers Communications | One Mount Pleasant Road | Toronto ON M4Y 2Y5

Identifying Expired Implied Consent Under CASL

CASL has specific requirements concerning how long implied consent is valid, as such the **date** when the business relationship ends must be used to calculate a **consent expiry** date to ensure Rogers **does not** send CEMs to individuals 24 months *after* the relationship ends.

