Apathy Let Cambridge Analytica Abuse 50 million Facebook Accounts

It was revealed last week that Cambridge Analytica abused personal information from 50 million Facebook accounts in early 2014 to build a system to profile individual American voters for the 2016 presidential election. The goal was to then target the users with personalised political advertisements attacking Hilary Clinton and loving The Donald. It's still not clear whether this was illegal or merely repugnant.

Most people are focussing on the fact that Cambridge Analytica was headed at the time by Steve Bannon, which provides yet another malodorous link to Trump. Facebook's share price is down about 12% but so far there has been no accountability apart from the inevitable class action litigation lawyers circling. What matters the most here is that we are becoming de-sensitized to data breaches like this.

$300M of Etherium permanently lost. Hey, it's just crypto and it wasn't mine, so who cares?

Do you know anyone who lost sleep over 143 million Americans and 100,000 Canadians that were exposed by Equifax's massive data breach.

Every Yahoo account was compromised in 2013, which Yahoo did not figure out until 2017. That was 3 billion accounts. You likely had one of those accounts. Did you complain about it?

Citibank failed to protect the personal data (including birthdates and Social Security numbers) of approximately 146,000 customers who filed for bankruptcy between 2007 and 2011. That's adding insult to injury.

40 million Target customers were exposed in 2013. The remedial cost to Target, not including the class action litigation, was roughly $252M. Did you join the class to get your rightful piece of the settlement?

$81 million stolen from the Bank of Bangladesh by compromising the Swift system in 2016. This was the second time Swift was used as a medium of theft. But hey, that could never happen over here in the civilized world, right?

Look at the lists here and here and here for some of the largest data breaches of all time. How many of these do you remember, or care about?

Even worse, according to the Online Trust Alliance in its terrifying *Cybersecurity and Breach Trends Report* from January of this year, is that 93% of these breaches were self-inflicted and easily preventable. Apathy is our real enemy.

And next up are the assaults from Artificial Intelligence.

AI spans a broad area. A Nest WiFi-enabled thermostat can self-regulate if it feels the sun directly on it rather than air in the home environment – is that 'intelligent' or just good programming? Cruise control on your car? A video game that gets harder the further you go and that learns your favourite moves? Neural networks? Deep learning? The hated robo-advisor? Predictive weather analysis? Smart tokens in the ICO universe?

AI is just a software operating in a hardware environment, but somehow it has gained noble status. Perhaps it's the use of the word "intelligence" that lulls us into thinking that the software is actually alive.

It's not. It's just software, a compendium of zeros and ones that open and close circuits inside chips. Software is vulnerable to coding errors, intentional or negligent. It's vulnerable to breakdowns in its hardware. And it's entirely

vulnerable to malicious third parties for cryptojacking.

Our courts and insurers will have to address who becomes liable when those things go wrong. The worse situation is where software causes death, like earlier this week when a self-driving car killed a woman in Tempe, Arizona. Elaine Herzberg was walking her bicycle when she was hit by a vehicle in autonomous mode going 40 km/h. It doesn't take a crystal ball to see Mr. Herzberg is the first of many such deaths.

Who will carry the financial burden of the error when smart tokens co-ordinate a contract for one billion rolls of toilet paper when the intention was for 100 rolls of paper towel? Is this contract law or negligence? Can you contract out of liability? Medical diagnostic software misses an obvious cause resulting in patient death? Who pays the repair bills when Skynet finally goes live and the Terminator kicks in your door?

Vernor Vinge's 1993 short paper *The Coming Tehnological Singularity* is a marvel of literature that manages to inspire and terrify at the same time. Should something we created actually develop its own intelligence, the pace at which technology would from that point develop would be inconceivable to humans. The human era would be over.

Back to the breaches, both malicious and self-inflicted. Incompetence and thievery have been with humanity for recorded history. The first trojan horse was the serpent surreptitiously attacking the Old Testament God by way of his human creations and an apple. Sadly, we do need various levels of government to help us defend ourselves. This will require some levels of regulation, even if unwanted.

The CryptoCrowd may not like it, but regulation is needed and it's coming. At least there seems to be some regulatory recognition that data is a different world requiring a different set of regulatory parameters. See for example the

British Columbia Securities Commission's 2018 outreach efforts seeking innovation while maintaining confidence in the capital markets.

This apathy is a strange mindset, especially since the business world otherwise takes confidentiality seriously. We sign confidentiality agreements and NDA's. We expect our employees to leave our IP at the office. Securities laws exist to prevent insider trading and to protect the dignity of the market. Larger boards have committees specializing in privacy and data protection. There are few things more valuable to any company than the integrity of its data.

So we should be outraged by these ongoing assaults on us, our data and our companies. We should be in the streets, with torches and pitchforks, demanding that heads roll and attackers be found. Instead, we shrug and say "What can we do? I'm just one helpless person. The government will protect us." That only goes so far.

We have to use what the government gives us. CASL (Canada's AntiSpam Legislation) is a horribly mis-named piece of legislation that has teeth. It codifies an individual's right to control the inbox. It isn't about spam, it's about your digital liberty.

The GDPR is the European Union's approach, and it's a good one. A prior article explaining GDPR is here. Recent recommendations from House of Commons Standing Committee on Access to Information, Privacy and Ethics indicate that Canada will adopt an approach similar to GDPR to give you the tools to protect yourself. So use them.

Ultimately, it's up to you. Be vigilant. Protect your local network. Follow good protocols. Don't be sloppy. And be angry over every breach. Demand accountability. Next time it could be you.

The CRTC could use Big Chicken for CASL

Morgan Spurlock is back! You'll remember Spurlock from his 2004 documentary *Supersize Me*, where he combined sharp film-making skills with performance art in eating nothing but food off the McDonald's menu for a month. His dramatic weight gain and precarious decline in health over a mere 30 days of fast food offered a shocking real-world commentary on our everyday lives.

Now he's back, with *Supersize Me2: Holy Chicken* which premiered at the Toronto International Film Festival this week. This time, his work looks at the chicken industry, and more particularly, the words used by "Big Chicken" to convince the public that it's healthy to eat fried chicken and reformulated chicken bits.

Big Chicken's marketing approach is based on its use of language to change our behavior. Health-conscious consumers now avoid "deep fried chicken", so instead they call it "crispy" or "grilled", because that sounds healthier. A crispy chicken sandwich is just deep fried chicken in a sandwich, but it sounds so much healthier now. Big Chicken uses "free range" to conjure up images of blissed-out chickens clucking through natural fields of abundant food; in reality all it means is that a door was left open on the enclosure to give the chickens the option of going into another small enclosure, even if none of the chickens actually left the crowded living area.

Have you heard any advertisements that chicken is "hormone free". Of course it is! The use of hormones is illegal in the

industry so all chicken you eat is hormone free, but again, the language is meant to shape our behaviour.

I wish someone in the Big Chicken industry would go to work for the CRTC.

The CRTC is Canada's Radio-Television and Telecommunications Commission. It was created in 1976 to regulate broadcasting and telecommunications, and its jurisdiction has crept into the enforcement of internet-related regulatory issues, which means the CRTC is the primary body enforcing *Canada's AntiSpam Legislation* (CASL).

The CRTC has been enforcing CASL since CASL came into force in July, 2014. Throughout the transition periods the CRTC did a good job of communicating with the public. It educated us as to what was expected to be in compliance, toured across the country to meet with stakeholders, gave some idea of what the penalties would be for non-compliance, and followed through with enforcement activity. The CASL enforcement division of the CRTC was generally a responsive public-friendly group, with a useful informative website.

The CRTC then named the violators, punished them, and advertised the results so as to shape the behaviour of everyone subject to the law.

The system was working.

Then the CTRC got blindsided by Navdeep Bains. Mr. Bains, who is Canada's Minister of Innovation, Science and Economic Development, gutted the CRTC's CASL process, in response to pressure from self-interested lobby groups. For a full explanation of what he did and why it was a disappointing failure of leadership, click here.

Since then, we've heard nothing from the CRTC on its CASL approach. The usually public-friendly department has gone radio silent, not even responding to my telephone and email

requests for guidance on future compliance.

Whether you approve of CASL or you hate it (and I recognize the haters far outnumber the approvers), it is the law of the land and it must be obeyed. The CRTC is the primary regulatory charged with its enforcement, both within Canada and internationally. As people subject to that law, we have the right to know the CRTC's interpretations of some of the murkier sections, how it will enforce breaches, how it will integrate CASL with the new privacy and data laws in Canada and abroad, and what is its overall theme on CASL.

To not give this guidance is unfair to everyone subject to the law (that is, everyone who sends email), to the lawyers who are trying to advise on it, to the auditors trying to assess risk related to it, to Human Resources trying to build employee compliance, and to third parties who have built businesses on CASL compliance.

Big Chicken has figured out that the language used can be more important than the substance of the thing being discussed, and that how we describe things can change behaviour. The CRTC needs to return to its public-friendly approach so that we know how to behave to stay within the law. Crispy chicken, anyone?

Feds Fail Canada on CASL

The law of Canada since 2014, Canada's AntiSpam Legislation was intended to clean up Canada's digital highways by empowering the owner of any email address to control what messages made it through to the inbox. This control was intended to make the overall economy more efficient. The CRTC has been enforcing CASL with a variety of tools including a

fine against one company for $1.5 million.

The private right of action under CASL was due to be effective July 1, 2017. Prior articles on CASL and the PRA can be found here and then going back through the hyperlinks.

This PRA was a key component of Canada's well-thought out strategy in the cyber world. As was written in the Report of the Task Force on Spam in 2005:

> *There should be an appropriate private right of action available to persons, both individuals and corporations. There should be meaningful statutory damages available to persons who bring civil action.*

With the July 1 date three weeks away, and the prospect of class action litigation against every company not in compliance, companies were finally taking CASL seriously and were sprinting to get Human Resources, Legal, IT and the executive offices working together to remediate the situation. The CASL system was working.

This week, 12 years after that report from its own Task Force, the federal government failed Canadians by derailing its own system. By order in council, the enactment of the PRA has been indefinitely delayed. There is no visibility on when or even if this part of the legislation will become active.

The team at the CRTC must be insulted by this political interference. The CRTC has done an effective job of regulation in this space, with one eye always on the July 1 PRA date as a motivating element. With one administrative pen wave, Minister Navdeep Bains gutted all of its hard work in education, lobbying and system-building.

Minister Bains was under pressure from various self-interested lobbying groups whose members failed to get in compliance, despite having years to do so. His decision to give in and

indefinitely delay the enactment of the PRA was an abdication of leadership.

So what's next? Remember when you were young, and your older sibling got in trouble with mom, then that sibling passed it on and took it out on you. Expect the same to happen here. The CRTC is in our opinion going to ramp up its enforcement efforts and pass on Minister Bains' insult to Canadian companies. We expect to hear of new enforcement actions by the CRTC under CASL over the next few weeks.

The PRA may not be in force but the rest of CASL remains the law of Canada, with the CRTC having incredible enforcement powers including the ability to obtain a warrant enforceable by the RCMP. Don't let your company be the target of that beating. Get into compliance with CASL by having IT, HR and legal work together under one responsible executive. This is a multidiscipline problem requiring a multi-department solution.

You can't count on the feds for leadership here so please do it yourself.

The CRTC War on Spam starts nailing the little man

This Man was Fined $15,000 for Sending Marketing Emails – CASL and the CRTC

You run your own business. You're not a corporation, you're just one person working out of your basement. Cash flow is a little tight so you need a little more revenue. You email a

simple marketing flyer to prospective customers. BOOM! The CRTC whacks you with a $15,000 fine.

Unlikely scenario? It happened last week to William Rapanos.

For the first time, the Canadian Radio-television and Telecommunications Commission (CRTC) fined an individual for CASL breaches, and if it happened to him, it can happen to you. The decision on the CRTC website is here.

Rogers Media, PlentyofFish Media, Porter Airlines, Kelloggs… all well-known corporate names that have been fined under CASL. The high-water mark is a fine of $1,100,000 issued to a numbered corp doing business as CompuFinder. Rapanos is the first human to be hit.

We've been warning of CASL (Canada's AntiSpam Legislation) and its potentially horrific consequences since prior to its enactment by the feds in 2014. There are two key components to CASL. Number one is that before you send a business email or text, you have to have that intended recipient's consent to receive that email or text AND you have to be able to prove you actually had that consent. Number two is that your emails must be transparent and contain an unsubscribe feature.

There are other sections and subtleties, but for today those are the guts of the statute.

What did Rapanos do to attract the CRTC's attention? He emailed an inoffensive marketing flyer, in which he advertised being able to design and deliver flyers through Canada Post. The email didn't include an unsubscribe feature or the other features required by the statute. Fifty people complained to the CRTC about receiving this flyer by email.

That's all it took, fifty complainers. The CRTC investigated. Rapanos was fined $15,000.

Granted, he didn't help himself. A notice from the CRTC is not

a casual document – it is the start of an investigation from a regulator who has shown a willingness to fight at street level (recall that the CRTC has already obtained two separate warrants under CASL, enforced by the police). Rapanos' response was that an unknown person hacked his router and the emails weren't sent by him. Trumplike, he offered no evidence for this bald assertion and so his defence failed. As the CRTC held, "It is highly improbable … that Mr. Rapanos was the victim of an identity theft orchestrated solely for the purpose of sending unsolicited [emails] advertising a flyer distribution business."

Think of the resources the CRTC must have dedicated to the investigation, prosecution and his appeal. Yes, Rapanos clearly breached the statute, but he's a small time offender. All he did was use the internet to offer his services to a new target market. Who did he offend in a previous life to earn this kind of bad karma? He's just a little guy.

And that, I think, is the point. This wasn't a knee-jerk reaction from the regulator, and it wasn't a random decision to prosecute him. Fifty complaints is a pittance. This was a carefully planned message, and that message is, no one is immune from CASL. Whether you're the size of media giant Rogers or a little guy like William Rapanos, CASL applies to you. You've been warned.

It will get worse on July 1, 2017. As we've pointed out before (most recently here) that is when a new private right of action (PRA) is created by CASL. In other words, if you send an email, and you can't prove you had prior consent to send it, the recipient can sue you. Then the onus is on you as the sender to prove you had prior consent to send it, not on the recipient to disprove it. This PRA supports class action litigation, and just to make it a full roundhouse kick in the groin, damages are assumed, which means the plaintiff wouldn't even have to prove damages to win.

This is the law of the land, from the Arctic Circle to the Great Lakes waters. The CRTC has made it clear that we are all subject to it.

This isn't an attack on the CRTC. Sure, that government body has messed up many times (follow Mark Goldberg on twitter @Mark_Goldberg for his frontline view of the CRTC's travails), but here, it's merely enforcing the law.

To their credit, the CRTC staff have done their best to warn us. They have toured the country holding information sessions, before the legislation was enacted and after. The website is full of useful, easy-to-read information. They have clearly communicated their intentions to the public. The CRTC also partnered with New Zealand to fight global spam. The problem is, the public hasn't been listening.

Rapanos was picked to force you to listen. Get into CASL compliance now so you're not the next one tied to the whipping post.

CASL – imposing fines to work.

What do the NFL Playoffs and CASL have in common? Freakonomics

Last September we looked at the NFL preseason, with the NFL imposing fines after the games for activities carried out during preseason play. The Commissioner's office wanted to shape behaviour and used monetary penalties to effect the change it wanted, before the regular season began.

At that time we said, "The NFL told its teams that it would be

enforcing the roughing rules more closely, and has followed through on that with financial penalties. Other players have to be taking notice and consequently changing how they play the game to comply with the rules."

Now the regular season is over and we're in the playoffs. The NFL is not levying those same fines, which leads one to believe the underlying behaviour has changed, meaning the financial penalties worked. The players are playing the game differently. Levitt and Dubner at *Freakonomics* would be impressed.

Freakonomics was an immensely influential book. Published in 2005, in addition to being fun and witty, it was one of the first books to bring data mining to the masses, showing how fresh looks at data can describe why people behave the way they do. Levitt and Dubner theorized that social, moral and financial incentives could explain why teachers cheated in Chicago, why the USA's national violent crime rate fell, why sumo wrestling in Japan is often as scripted as the WWE, and why good parenting could have minimal impact on a child's education.

Levitt and Dubner described the world as a system of intentional and accidental moral, social and financial incentives working as push/pull levers to shape behaviour. Their work is as much sociology as it is economics. But it's hard to argue with this theory, that incentives can cause us to change our behaviour.

This is the theory that has been embraced by the CRTC (Canada's Radio-Television and Telecommunications Commission). Created in 1976 to regulate broadcasting and telecommunications, the CRTC's jurisdiction has crept into the enforcement of internet-related regulatory issues, which means the CRTC is the primary body enforcing *Canada's AntiSpam Legislation* (CASL).

The CRTC has been levying Administrative Financial Penalties since CASL came into force in July, 2014. New rules governing computer programs came into force the following January. The CRTC has named the violators, punished them, and advertised the results so as to shape the behaviour of everyone subject to the law. The CRTC has even obtained two warrants to enter business premises to enforce CASL.

Visit the CRTC's website here for the statute itself, the regulations, and the penalties already levied. The CRTC has defined the high standards it expects to be observed, and has made it clear that it won't take violations lightly.

The NFL might be in the playoffs but CASL is just finishing its preseason. The regular season begins July 1, 2017.

That date is when a new private right of action is created by statute. In other words, if you send someone an email, and you can't prove you had prior consent to send it, the person receiving that email can sue you. The onus is on you as the sender to prove consent, not on the recipient to disprove it.

Even worse for the sender of email, damages are assumed, which means the plaintiff is assumed to have been monetarily hurt by receiving an unwanted email. Further, this private right of action supports class action litigation.

If you want to research the basics of CASL and why your highly-paid defence lawyers will be very happy you're not in compliance, go here. Please note this doesn't apply only to what is typically thought of as 'spam'; CASL applies to every email and text message you send.

Are you ready for CASL's regular season? As we've said before, the CRTC has made it clear that a CASL-compliant model includes:

1. a senior executive to champion the creation and implementation of your compliance model

2. a senior executive to supervise compliance and respond to potential breaches
3. Human Resources to add sections to the Employee Handbook on the proper use of email addresses and phone numbers
4. initial training of all staff, directors and management
5. annual testing to ensure continued compliance
6. a technology model that has been architected to achieve all the business goals set out in CASL and as interpreted by the CRTC
7. initial and on-going stress testing of the system

The incentives are in place to shape CASL-compliant behaviour. Perhaps CASL and its impacts can be a chapter in the next instalment of *Freakonomics*.

The CASL Fines are Starting to Pile Up

The CRTC recently rolled out another conviction under CASL.

Here are the barebones of CASL compliance from a video interview last January:

CASL is a piece of legislation with good intentions. It's meant to enhance Canada's economy and increase efficiencies by eliminating waste. That sounds great. What the government has done is passed a law that says if you send an electronic message to another person's account you must have that person's consent before you send that message. Notice it doesn't say email. It says electronic communication. Notice it doesn't say email account. The legislation reads, to an account. As a result it is so broad, so encompassing, that it catches every aspect of your business.

After talking about it since 2012, it was about a year ago that we started emphatically writing about Canada's AntiSpam Legislation ("CASL"), when we wrote, "it is by far the most pernicious legislation I've ever seen."

In another article we called it "corporate ebola" and elsewhere said that it poses a tremendous uninsurable risk for every business sending or receiving email in Canada.

We also warned that under CASL the CRTC (Canadian Radio-Television and Telecommunications Commission) had the power to obtain warrants, enforceable by the Royal Canadian Mounted Police. We can't think of anyone who took it seriously at the time. They did when the CRTC obtained and enforced two warrants under CASL. Suddenly businesses were paying a bit more attention.

Other companies have treated CASL casually, and paid a hefty price. Look at CompuFinder (fined $1,100,000 for CASL infractions), Porter Airlines ($150,000), Plenty of Fish ($48,000), Rogers Media ($200,000) and Kellogg's ($60,000).

From inside sources we know that Rogers' legals for internal and external counsel was roughly $2,000,000, not including lost time and the resources then consumed by an after-the-fact compliance effort.

Look at the article here for background and links to prior articles spelling out what CASL is, what its requirements are, and why it will be extremely difficult to comply without a management-led attack on the issue.

The CRTC has told us it will enforce CASL to exacting high standards. An Enforcement Advisory published earlier this year described those very high standards.

That's all background. On October 26, 2016, the CRTC found that Blackstone Learning Corp. committed nine violations of CASL by sending commercial electronic messages without

consent, and imposed an administrative monetary penalty (AMP) of $50,000 on the company. The really scary part was that in the original notice of violation, the CRTC was seeking a AMP of $640,000. Six hundred and forty thousand dollars, for sending business emails.

Scary.

So picture Blackstone getting that Notice of Violation. Its board of directors had a difficult decision to make: pay the $640,000 AMP, or pay its lawyers a crippling amount of money to fight the CRTC in the hope of having that AMP reduced to a manageable level. I don't know how much Blackstone paid, but I do know the legal industry, so my guess is the legals for this process were at least $300,000. Not an easy decision.

Blackstone sent emails primarily to government employees, advertising educational and training services offered by the company. The employees complained to the CRTC that they had not consented to receiving those emails. The onus was then on Blackstone to prove to the CRTC that it had prior consent to send the emails. Since Blackstone could not prove on a balance of probabilities that it had express or implied consent, the CRTC found Blackstone guilty.

The Blackstone facts also addressed the internet practice known as "scraping". Also known as "web harvesting" and "web data extraction", scraping is an automated process that extracts information from thousands of websites. In this context, the target information is all email addresses posted at that website, and then the scraper will use that contact information to market its services to those email addresses. How those publicly posted email addresses can be legally used is called "the conspicuous publication exemption".

For the first time, the CRTC offered a detailed analysis of the "conspicuous publication exemption" found in section 10 (9)(b) of CASL. That's the good news, as it provides guidance

and some certainty for compliance departments and Heads of Risk. The bad news is, the CRTC interpreted the exemption fairly narrowly, which guarantees future violations.

Here's the CRTC's own words from section 28 of the reasons:

Paragraph 10(9)(b) of the Act does not provide persons sending commercial electronic messages with a broad licence to contact any electronic address they find online; rather, it provides for circumstances in which consent can be implied by such publication, to be evaluated on a case-by-case basis. Pursuant to section 13 of the Act, the onus of proving consent, including the elements of implied consent under paragraph 10(9)(b) of the Act, rests with the person relying on it.

In its reasons, the CRTC did knock down the AMP to $50,000 from its initial $640,000, but think of the incredible legal fees Blackstone had to incur to achieve that. And that's the reason we get so worked up about CASL; it's not the potential for fines, it's the staggering legal costs involved in defending a Notice of Violation. There aren't many companies that can digest millions of dollars of uninsurable legal fees.

And it's going to get worse. As of July 1, 2017, the CRTC isn't your worry. As of that date, a private right of action will be created, which means that anyone can sue you and allege that you breached CASL. Then, as the CRTC pointed out in *Blackstone*, "the onus of proving consent … rests with the person relying on it."

That private right of action is supportable by class action litigation, with plaintiff lawyers working on contingency. Meanwhile, the legal defence fees will be in the millions of dollars.

It's cheaper to get into compliance than to pay your lawyers. Get into compliance with CASL now.

PreSeason, the NFL and CASL

The NFL is trying to clean up its thug image and, after the notoriety following Will Smith's 2015 movie Concussion, is working hard to eliminate public perception that it doesn't care about the physical well-being of its athletes.

Kerry Hyder is a defensive end in the Detroit Lions training camp, battling for a roster position. He's been here before, in other training camps for other teams, trying to finally land a full-time football job. In venture capital terms, Hyder is post-startup but still minimal-revenue.

The National Football League recently fined him over $18,000 for roughing Cincinnati Bengals quarterback AJ McCarron in the third quarter of a relatively meaningless preseason game on Aug. 18. The play was so mild, so innocuous, that I can't find video of it. It was just a normal part of an average boring preseason game, resulting in no injury, no victim, no ugliness, but yet, the regulatory body imposed a fine on the player after the game. He's only making $1,000 a week during the preseason.

He's not the only player to be fined this preseason by the NFL. Two others (Houston's John Simon and the Seahawks Jarran Reed) were also fined for similar roughing infractions. Just in Week 1 of the preseason, seventeen players in total were fined for onfield play.

The NFL told its teams that it would be enforcing the roughing rules more closely, and has followed through on that with financial penalties. Other players have to be taking notice and consequently changing how they play the game to comply with the rules.

There are direct parallels between Hyder and your business. Think of the CRTC as the NFL. Think of all your daily electronic business communications as the game. And now, think of CASL as the rules the NFL-CRTC has told you it will enforce.

The CRTC (Canada's Radio-Television and Telecommunications Commission) was created in 1976 to regulate broadcasting and telecommunications. It reports through the federal Minister of Canadian Heritage to Parliament. Enforcement of internet-related regulatory issues has grown into its area of jurisdiction, which means the CRTC is the primary body charged with enforcing *Canada's AntiSpam Legislation* (CASL).

There is considerable background on CASL in this article with links to prior articles on what CASL is, why it exists, what are the basic requirements and why July 1, 2017 is going to be a terrible date for business. Please go back to those for context. We have repeatedly pointed out that the biggest CASL financial cost to a company will be its lawyers, with the actual fines being imposed by the CRTC coming second.

The CRTC has told us it will enforce the rules as written, and has told us what standards are expected of us. The Enforcement Advisory published earlier this year described the high bar that compliance with CASL must hurdle over. There will be fines levied for failure to comply.

In case you think you can ignore CASL, ask CompuFinder (fined $1,100,000 for CASL infractions), Porter Airlines ($150,000), Plenty of Fish ($48,000) or Rogers Media ($200,000) what they think. Inside sources have told us Rogers' legal bills for internal and external counsel was roughly $2,000,000, not including lost time and the resources then consumed by an after-the-fact compliance effort.

To that list we can now add Kellogg Canada Inc. Kellogg's, whose brands include Froot Loops, Special K, Pop-Tarts, Corn

Flakes, Eggo and Rice Krispies, was fined $60,000 in August, 2016 because, “from 1 October 2014 to 16 December 2014, inclusively, messages were sent by Kellogg and/or its third party service providers … to recipients without consent of their recipients.” (from the CRTC’s webpage).

That CRTC investigation has been underway for some time. How much do you think Kellogg’s has paid to its lawyers to deal with this?

Just as the NFL followed through on its rules enforcement, so too is the CRTC. The Supreme Court of Canada in *Guindon v Canada* in 2015 said that Administrative Monetary Penalties (the fancy-pants way of saying “a fine”), the kind the CRTC can levy under CASL, are a valid part of the legal landscape, so expect to see further fines and settlements as other investigations wind their way through the system.

…and it’s only going to get worse!

As of July 1, 2017 (a mere ten months from now) CASL infractions will give rise to a private right of action, supportable by class action litigation. Anyone to whom you send an email or a text can sue you, and then the onus is on you to prove you had consent to send that message. Whether you had consent is irrelevant under CASL – you have to be able to prove you had that consent. So look at your record-keeping: could you prove that today? If not, you are not CASL-compliant and your business is at risk.

It doesn’t matter that you may think the law is silly, disproportionate or inapplicable: it exists and it applies to you. How much do you want to pay to your lawyers and the plaintiffs’ class action lawyers? Wouldn’t it be cheaper to simply comply with CASL?

Kerry Hyder’s play on AJ McCarron was innocuous but was outside of the clear rules of the game, resulting in a direct penalty imposed by the regulator. The same thing is happening

with the CRTC and CASL.

We are in CASL’s preseason. The real season begins July 1, 2017. Learn the rules and play within them to avoid serious penalty.