Volume 03, Issue 01

Summer 2015

## Inside This Issue



# The PARTNER

Northeastern Protection Service
Summer 2015 Newsletter

Like us on Facebook

Follow us on twitter
@NortheasternPro

www.protectionpartner.ca

# New Business

## Moncton Airport, TCL, and SMU

At Northeastern we are thrilled to have our largest client list in our 32-year history! To keep you all up-to-date, here are a few highlights of new business we have gained since our previous newsletter:

First up is the **Greater Moncton International Airport (GMIA)** in Moncton, NB. We are in the first year of a multi-year contract with GMIA, and we enjoyed a smooth transition thanks to the dedication and cooperation of our valued employees! Northeastern brings years of experience in aerospace security to GMIA and we are excited to have this strong presence in the New Brunswick market after a brief hiatus.

Next up is **Trade Centre Limited (TCL)** in Halifax, NS. Northeastern has been granted status as an approved supplier for TCL and we have already begun providing event security at the World Trade Centre as well as the Scotiabank Centre in Halifax. We have worked events such as *Stars on Ice*, *The Counting Crows* concert, and other exciting functions. There will be much more to come in the future!

In June of this year, we entered a multi-year contract with **Saint Mary's University (SMU)** in Halifax, NS. Northeastern was the winner of a competitive bid process which involved all of the major security firms in the region as well as national and international companies. Thanks to our organized security staff and management team, the transition was successful and we are looking forward to providing services to the staff, faculty, students, and visitors of SMU in the years ahead!

# Amalgamation of companies

## Northeastern group of companies now amalgamated

At our inception in 1983 "Northeastern Investigations" was our registered company name in Nova Scotia. It became incorporated in 1988, and was subsequently registered as an extra-provincial corporation in several Canadian Provinces. As our services expanded to include uniformed guards, technical security systems, and ID systems and supplies, we decided to register "Northeastern Protection Service Inc" to better represent our range of physical security services. In the meantime we had also registered a numbered company to manage some real estate investments "3101570 Nova Scotia Limited". We realized that as we grew and changed, we had perhaps created some branding confusion!

To address this, we applied under the Corporations Registration Act of Nova Scotia to "amalgamate" all of these companies under one banner; *"Northeastern Protection Service Inc."* This occurred August 1, 2014. Having the one company now streamlines our back office administration and simplifies our branding efforts moving forward.

# Have we forfeited our privacy?

By Roger Miller

***Recent discussions surrounding the federal government's Bill C-13*** focused on the access to personal data by law enforcement or other government agencies; personal data really means our private information.

Within the discussion at many levels was the effort to bring cyber-bullying into the conversation. This is relevant to security managers on a very real level. Although much of this debate has surrounded two high-profile deaths of teenagers, it will affect us at the corporate level as well as the personal level.

However, is enforcement within the authority of an Act of Parliament the best approach to protecting Canadians from the insecure world of on-line risks? Let's compare this crime to other more visible criminal activity. For more than 40 years the government has spent untold dollars educating Canadians about the dangers of, and how to report, drug activity. Prevention through education has been a major focus of the efforts to attack serious crime. This is where Canada along, with other industrial nations, must go. Unlike the drug trade that a person would willingly enter as a consumer, everyone has a risk of being a victim of cybercrime. Regardless of whether or not you use the Internet there is electronic data on you out there that you have no control over. This data is not only held by government, there are business partners, employers and even your favourite coffee shop storing your personal data.

A typical Canadian daily routine goes something like this;

- *Check your e-mail / Facebook / LinkedIn/ Twitter accounts*
- *Leave home and stop for coffee*
- *Buy gas*
- *Travel through toll highway / bridge*
- *Transit system*
- *Check your e-mail / social media accounts (again)*
- *Lunch*
- *On-line purchases and on-line banking*
- *Check your e-mail / social media accounts (again)*
- *Return home*

## Have we forfeited our privacy? (*continued from page 2)*

Each of the above activities is electronically recording your presence. CCTV, debit or credit card transaction, IP addresses and GPS recording is taking place in an intrusive manner that you cannot control. You can opt *not* to do business with a company because they are recording your personal information, but realistically there are no options that will completely eliminate this activity. Therefore we need to educate all citizens regarding the digital footprint they are leaving, with or without their knowledge and consent.

On the corporate level executives need to be educated on what information their company is gathering, how it is stored and what it is used for. Ultimately they may be held accountable if there is a breach of personal data. Winners, Target and other major retailers have suffered significant breaches and their executives have paid a price for it. Although this topic has been on the table for some time the message has not been clear. The following is an excerpt taken from the federal justice website:

*"Bill C-13 would reclassify certain powers and fix gaps in investigative tools. Production orders for transmission data and tracing of specified communications would be included in the Bill as new categories. These orders would adopt the judicial authorization threshold that is consistent with the existing specific production order powers, production order for basic financial data such as an account number, given the lower expectation of privacy in relation to such data."*

The above paragraph references "basic financial data" – When one considers what could fall under this context, it becomes a large pool of data on individuals or groups that many organizations collect and retain. Could basic financial data be stretched to determine how much fuel you purchase each month at your local service station or the credit information you supplied your local utility provider to set up your account? Could it be part of some detail you posted on Facebook? I believe it could and has been defined in those terms.


Protecting this data will be a key part of a Threat Risk Vulnerability Assessment for the foreseeable future. Security management must be closely aligned with the peripheral managers (IT/Privacy Officer) to provide a cohesive protection platform. Historically police agencies have had direct contact with security managers of larger organizations, the two parties would communicate on a regular basis. When the police needed information they would contact that security manager, often times no warrant or formal request was provided or requested. The justification for not formally requesting the information was almost always that the information was being shared in the interests of public safety. Good or bad, the dialogue surrounding Bill C-13 has heightened the awareness of just how much data could be shared about each of us.

From the coffee chain to the financial institution we deal with there is a tremendous amount of data out there to be shared. Someone has to manage that data internally for each organization because the request for the data from law enforcement or others will be coming. Asset protection has to be redefined to include this electronic data. Drawing a line that connects the death of teenagers to the Boardroom door isn't a farfetched concept. It is all connected to the privacy of Canadians and the responsibility everyone has to manage it. Without that knowledge, enforcement is going to be a very steep uphill battle for us.

Regardless of who holds our personal information, government or private industry, our privacy as we knew it is gone.

*Roger Miller is the president of Northeastern Protection Service Inc. and a Certified Identity Theft Awareness Trainer.*

# We'd like to hear from you!

## Northeastern Protection Service Inc.

Corporate Office:
202 Brownlow Avenue, Unit LKA1
Dartmouth, NS B3B 1T5
Phone: 902-435-1336
Fax: 902-435-0093

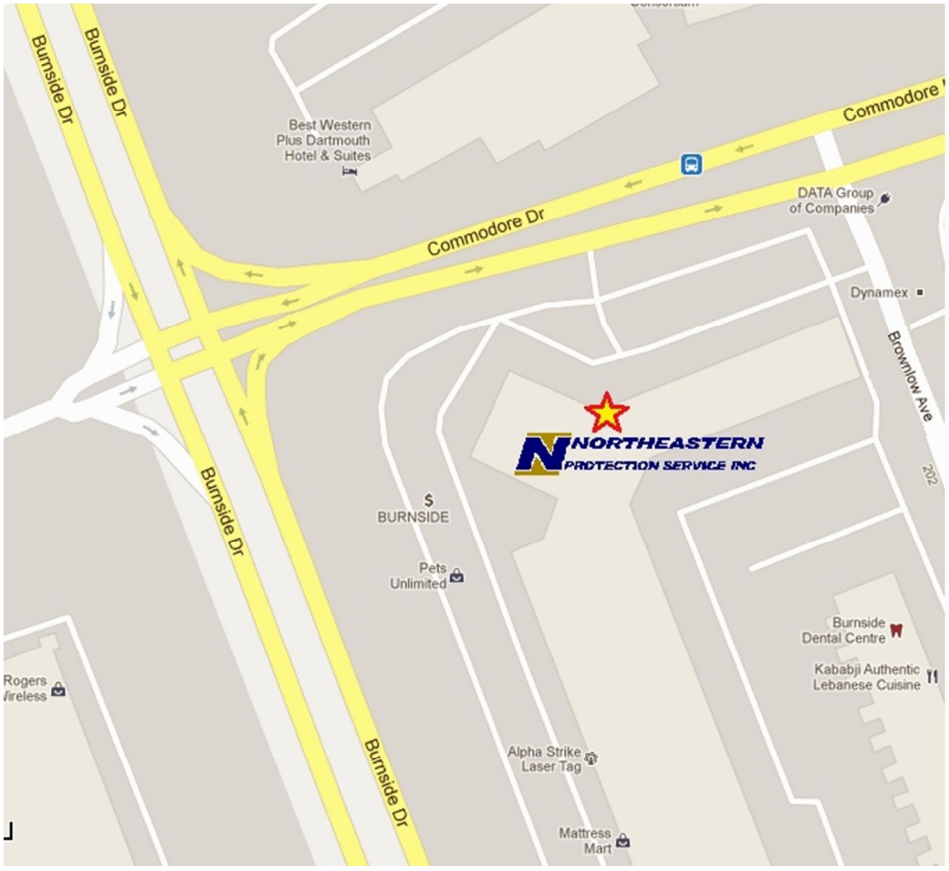
E-mail: info@protectionpartner.ca

Online: www.protectionpartner.ca/contact-information

Like us on Facebook

Follow us on twitter
@NortheasternPro

Visit us in Burnside Park, Dartmouth, Nova Scotia.
Near the corner of Burnside Drive and Commodore Drive




***Your Protection Partner™***