**Canadian Association of Chiefs of Police**
Leading Progressive Change in Policing

**L'Association canadienne des chefs de police**
À l'avant-garde du progrès policier

# Electronic Crime Committee 2012 Annual Report

CACP
E-CRIME
CANADIAN ASSOCIATION OF CHIEFS OF POLICE
ASSOCIATION CANADIENNE DES CHEFS DE POLICE
iStockphoto
COMMITTEE

# TABLE OF CONTENTS

# 2012 MESSAGE FROM THE CO-CHAIRS

The 2011/2012 CACP E-Crime Committee Activities Report reflects the objectives set out in the 2009-2012 Strategic Plan. The Plan is our road map which ensures that our efforts align with the overarching goals and objectives of the CACP.

Looking forward to 2013-15, the E Crime Committee is positioning itself with a new strategic plan that aligns its goals with the objectives set forth at the CACP President's Council in January 2012. Continued efforts are favoured to liaise and support other CACP Committees to promote a coordinated effort in combating cybercrime.

Over the past year, the E-Crime Committee has come to the conclusion that without an adequate reporting scheme to evaluate the seriousness, magnitude and pervasiveness of this problem nationally (corporate sector, banking sector, and in the general public), our ability to articulate an appropriate police response is seriously limited. Reliable data is crucial for police executives and public policy makers to effectively align resources to address what we believe to be an increasing threat. Consequently, this committee believes that the CACP should support a national harmonized data collection point for Cybercrime complaints / incidents.

Members of the committee have embraced the opportunity to actively participate in Canada's Cyber Strategy 2010 situation analysis endeavour being led by the RCMP. Our members believe the CACP should support the requirement for a National Cybercrime Strategy to disrupt and neutralize Canadian-based cybercrime, through means centered around:
a) The development of interagency capacity for increased coordination and collaboration;
b) The identification of inter provincial and international operational plans to increase the effectiveness of law enforcement initiatives;

With the explosion of social media and new communication tools available to users we need to understand the technology and how data collection/retention can be exploited. The E Crime Committee believes that new opportunities must be seized by the policing community to enhance our ability to intervene at the most opportune time to better serve our communities. The Committee members monitor new technologies; embraces new approaches, and evaluates new tools and initiatives within the prism of Canadian Law.

The Committee's current composition of Canadian police leaders, private sector special advisors, prosecutorial experts and technical advisors provide a vast array of knowledge and skills that position the committee well to achieve its objectives. The Committee membership includes police representatives from the RCMP, OPP, Sûreté du Québec, as well as Toronto, Ottawa, Montreal, Saskatoon and Edmonton Police Services. Related judicial representatives include members from Justice Canada, Public Prosecution Service of Nova Scotia, and the Crown Law Office of Ontario. Additional support is provided by the Canadian Police College who increasingly provide training efforts in this highly technical field. Private sector representatives, include the Canadian Bankers Association, Society for the Policing of Cyberspace and Microsoft Canada.

The E-Crime Committee held two meetings this year along with a teleconference. Meetings were held in October 2011 and May 2012 the meetings were held in Quebec City and in Edmonton, respectively. The teleconference was held on April 4, 2012. This realignment of committee activities was endorsed last fall at our Quebec City meeting in an effort to better coordinate the committee work of the subcommittee (National Technological Crime Advisory Sub-Committee) and achieve a better synergy between both committees. The new format allows for a joint meeting that overlaps both committees' schedules. This enables members of both committees to be exposed to the same information and share views on joint concerns. A third 'virtual meeting' was held in March 2012 to follow up on the committee work of respective members in preparation for the annual report. This formula was reflected on at our final meeting and was perceived as an enhancement of our core committee work.

This year the Committee pursued opportunities to provide strategic leadership in matters related to Internet governance. Committee members from the RCMP and la Sûreté du Québec supported representation at Internet Corporation for Assigned Names and Numbers (ICANN), American Registry of Internet Numbers (ARIN) and Internet Protocol Version 6 Working Group (IPV6WG) to voice concerns and needs of the law enforcement community. The ability to access reliable data in a timely fashion is at the centre of these concerted efforts with our international partners. Our representatives have sustained this effort to promote WHOIS due diligence recommendations to ICANN. Other initiatives supported a compliance resolution at the ARIN level and a proactive role of the IPV6 implementation drafting at the Internet Engineering Task Force (IETF) level and through the IPV6 WG.

The development of national standards in relation to electronic crimes is an on-going activity of the Committee. The Committee wishes to better promote the understudy program that was endorsed last year. Additional work on this issue is being communicated to the CACP membership through an article in the CACP Journal.

This year the Committee has worked with the CACP National Technological Crime Advisory Sub-Committee to advanced work in relation to interagency cooperation; triage tool development; discussions on forensic principles, improved and more flexible CPC training; evaluation of efficient cost reducing training alternatives through Web training programs. We expect that this work will continue into 2012/2013.

There are a number of emerging challenges in relation to electronic crimes and Canada's police services must work together to develop a coordinated, effective response. In 2012, the E-Crime Committee continued to be an excellent venue to share knowledge, skills and abilities to enhance strategies in combating E-Crime.

Committee members were provided with timely information bulletins from international policing partners in regard to emerging cyber-crime trends and threats. The E-Crime Committee and the National Tech Crime Advisory Committee ensure that leading edge information, training, technical tools, best practices and techniques are shared effectively with Canadian policing services. The Committee members agree, even during this period of fiscal restraint, that there is a requirement to ensure that new funding initiatives by all levels of government include sufficient allocations for specialized technical investigative services. These are complex and highly sophisticated investigations that require extensive training, travel and infrastructure support to provide an effective deterrent and to be able to investigate traditional and newly emerging crime trends. The E-Crime Committee continues to work to identify electronic crime investigation and prosecution issues to government and police leaders, provide options for change and exploit opportunities to enhance community safety.

The law enforcement members of the committee would also like to thank our private sector members, not for profit society members and government partners for their continued participation, support and ongoing efforts in combating cybercrime.

Superintendent Tony Pickett
Royal Canadian Mounted Police

Lieutenant Martin Charette
Sûreté du Québec

## Committee Mandate/Objective

e crime
committee
CANADIAN ASSOCIATION OF CHIEFS OF POLICE
ASSOCIATION CANADIENNE DES CHEFS DE POLICE

"To establish a leadership role in the development of an administrative policy and standards for technology-based investigations, including the promotion of inter-agency cooperation in the prevention, detection and investigation of internet-based crime, the establishment of training standards, the identification of effective cooperation strategies to combat e-crime at local, provincial, national and international levels and facilitate public education on information security."

# DATES/OVERVIEW OF MEETINGS

The e-Crime Committee meets in the Fall to identify goals and objectives. The Committee then aims to hold a teleconference in the early part of the New Year to further discuss objectives/initiatives and to determine an appropriate action plan for these items. A Spring meeting is then held to ensure action items have been addressed. The Committee members who participate in the meetings are supported by their respective organizations. CACP Board of Directors provides funds to offset certain expenses.

## Fall 2011
## NTCAC & CACP E-Crime Committee Meeting
## October 5-7, 2011
## Québec City, Québec

**Participating:**

| | |
|---|---|
| Tony Pickett (E-Crime Co-Chair) | RCMP – Ottawa |
| Martin Charrette (E-Crime Co-Chair) | Sûreté du Québec |
| Francesco Secondi | Service de police de la ville de Montréal (SPVM) |
| Louis Jacob | Sûreté du Québec |
| Il Kim | Sûreté du Québec |
| Francesco Secondi | Montréal SPVM |
| Jeff Mitchell | Peel Regional Police Service |
| Kevin Mallay | RCMP Nova Scotia |
| Jean-Francois Bernier | Quebec City Police Service |
| Danny Smyth | Winnipeg PS |
| Kevin Riel | Winnipeg PS |
| Grant Foster | Saskatoon Police Service |
| Paul Batista | Ottawa Police Service |
| Bill Bosward | Toronto Police Service |
| John Menard | Toronto Police Service |
| Joel Bautista | Saskatchewan ICE Unit |
| Craig Coughlan (Chair NTCAC) | Calgary Police Service |
| Dale Heinzig | Calgary Police |
| Phil Palamattam | Edmonton Police Service |
| Gareth Samson | Justice of Canada, Criminal Law Policy |
| France Thibodeau | Canadian Police College |
| Carole Matthews | OPP - Orillia |
| Marc Moreau | RCMP – Ottawa |

**<u>Regrets</u>:**

| | |
|---|---|
| Tom Fitzgerald | Toronto Police Service |
| Grant Foster | Saskatoon Police Service |
| Ray Archer | Canadian Bankers Association – Ontario |
| Ken MacKay | Edmonton Police Service |
| Bessie Pang | Society for the Policing of Cyberspace |
| John Weigelt | Microsoft Canada |
| Alexander Smith | Attorney General, Crown Law Office – Ontario |
| Dan MacRury | Nova Scotia – Public Prosecution Service |

Items discussed included:

- Overview of the Technological Crime Learning Institute, Canadian Police College. The Committee was asked to entertain the possibility of adopting a Resolution with regards to establishing a standard for child exploitation investigators
- Overview of the Canadian Police Centre for Missing & Exploited Children (CPCMEC)
- Overview of the RCMP Cyber Crime Analysis Team (CCAT)
- Overview of the RCMP Cyber Crime Fusion Centre (CCFC)
- Overview of the Internet Corporation of Assigned Names & Numbers (ICANN) and the American Registry for Internet Number (ARIN)
- Report on the last CyberStorm III exercise, September 27-30, 2010
- Survey from the Department of Justice on Pre-paid Cell Phones
- Next steps

Full Meeting minutes are available in **Appendix "A"** of this report.

## Spring 2012
## NTCAC & CACP E-Crime Committee Meeting - Teleconference
## April 4, 2012

The NTCAC and CACP E-Crime Committee held a teleconference on 2012-04-04 to discuss some of the following items (in preparation for the upcoming meeting in Edmonton, May 2-4, 2012): following is a Summary of our teleconference of 2012-04-04 at 14:00hrs.

**PARTICIPANTS**:

Supt Tony Pickett (Co-Chair), RCMP, Ottawa
Lieutenant Martin Charette (Co-Chair), Sûreté du Québec
Supt Ken MacKay, Edmonton PS
Commander Francesco Secondi, Service de police de la Ville de Montréal (SPVM)
A/Supt Ian Kingham, Ottawa PS
S/Sgt Carole Matthews, OPP
Detective John Menard, Toronto PS
France Thibodeau, Canadian Police College
Mr. Gareth Sansom, DOJ
Ray Archer, Canadian Bankers Association
John Weigelt, Microsoft
S/Sgt Marc Moreau, RCMP, Ottawa

**REGRETS (confirmed):**

Supt Grant Foster, Saskatoon PS
C/Supt Mark Fleming, RCMP "E" Div
C/Supt Ron Gentle, OPP
Supt Tom Fitzgerald, Toronto PS
Supt John Bilinski, RCMP. CPCMEC, Ottawa
Bessie Pang, Society for the Policing of Cyberspace
Dan MacRury, Nova Scotia - Public Prosecution Service

**Summary of discussions**:

Item #1: DOJ Questionnaire - Mr. Gareth Sansom, DOJ
Item #2: National Cyber Crime Strategy - Mr. David Black, RCMP, Ottawa
Item #3: Strategic Plan - Supt Tony Pickett, RCMP, Ottawa
Item #4: Training Opportunities - S/Sgt Marc Moreau, RCMP, Ottawa

Full Summary of this teleconference is available at **Appendix "B"** of this report.

## Spring 2012
## NTCAC & CACP E-Crime Committee Meeting
## May 2-4, 2012
## Edmonton, Alberta

**Participating**:

| | | |
|---|---|---|
| Tony Pickett | (Co-Chair) | RCMP – Ottawa |
| Martin Charette | (Co-Chair) | Sûreté du Québec |
| Louis Jacob | | Sûreté du Québec |
| Il Kim | | Sûreté du Québec |
| Francesco Secondi | | Montréal SPVM |
| Jeff Mitchell | | Peel Regional Police Service |
| Kevin Mallay | | RCMP Nova Scotia |
| Jean-Francois Bernier | | Quebec City Police Service |
| Danny Smyth | | Winnipeg PS |
| Kevin Riel | | Winnipeg PS |
| Grant Foster | | Saskatoon Police Service |
| Ian Kingham | | Ottawa Police Service |
| Paul Batista | | Ottawa Police Service |
| Bernard Murphy | | OPP - Orillia |
| Ken MacKay | | Edmonton Police Service |
| Stéphane Denis | | RCMP – Canadian Police College |
| Bill Bosward | | Toronto Police Service |
| John Menard | | Toronto Police Service |
| Joel Bautista | | Saskatchewan ICE Unit |
| Craig Coughlan (Chair NTCAC) | | Calgary Police Service |
| Dale Heinzig | | Calgary Police |
| Marc Moreau | | RCMP – Ottawa |

**Regrets**:

| | |
|---|---|
| France Thibodeau | RCMP - Canadian Police College |
| John Bilinski | RCMP – Ottawa |
| Carole Matthews | OPP - Orillia |
| John Weigelt | Microsoft Canada |
| Bessie Pang | Society for the Policing of Cyberspace |
| Ray Archer | Canadian Bankers Association – Ontario |
| Gareth Samson | Justice of Canada, Criminal Law Policy |
| Alexander Smith | Attorney General, Crown Law Office – Ontario |
| Dan MacRury | Nova Scotia – Public Prosecution Service |
| Tom Fitzgerald | Toronto Police Service |
| Kevin McQuiguin | Vancouver Police Department |

Items discussed included:

- Review of CACP Strategic Plan 2012-2015
- Search Warrants and Court Procedures
- Searching the Cloud

- Computer Emergency Response Team (CERT)
  - Virtual e-Learning opportunities
  - Live demo of virtual e-Learning
- Lawful Access Update
- Canadian Police College – Update
- OPP eTracker Demonstration
- Validation of tools
- Review 2012 Annual Report (submitted at the CACP conference in Windsor August 22, 2011
- Law Enforcement Due Diligence Recommendations to ICANN (Update in LE efforts to gain a voice in the Internet governance at the international level
- ARIN – Results of the recent Policy Proposal at the ARMIN meeting – Vancouver April 2012 (policy 2011-07 Compliance Requirements https://www.arin.net/policy/proposals/2011_07.html
- Discussion regarding 3 questions from the Cyber WG regarding encryption
- Next steps

Full Meeting minutes are available in **Appendix "C"** of this report.

# Summary of Initiatives/Activities 2011/2012:

- Supported efforts with international law enforcement at the Internet Association for Assigned Names and Numbers (ICANN) for adoption of law enforcement due diligence recommendations regarding Internet governance.
- Developed a resolution to develop a national Cyber Crime strategy
- Assessed emerging risks and potential for criminal exploitation of virtual worlds.
- Working with the Computer Emergency Response Team (CERT), Carnegie Mellon University to obtain access to much needed virtual training opportunity
- The Committee continues to work with the operational members of the National Tech Crime Advisory Committee (NTCAC).

# Resolution 2012-01

## National Cybercrime Strategy

### *Commentary*

Internet commerce and a complex array of computing devices have become essential to the way Canadians live and conduct business. Private and public sectors, critical infrastructure operators and the digital economy, in some way, now depend on cyber systems 24/7.

Unfortunately, crime goes hand–in-hand with this dependence and evidence of the harm caused is seen daily in media reports. Criminals, activists, hacktivists and Organized Crime, now use computers to commit a multitude of technological crimes, (e.g. service disruption, data or identity theft, hacking, intercept of communications, financial fraud, drug dealing, terrorist planning and more). Some of these incidents have resulted in arrests both domestically and internationally. These cyber threats quickly and easily target individuals or groups on a global scale.

In line with proposed new legislation, Canada's Cyber Security Strategy and the Council of Europe's Convention on Cybercrime, Canada must now articulate a comprehensive National Cybercrime Strategy in order to detect and disrupt this new wave of crime. The public's confidence in policing, critical infrastructure protection and public safety is paramount.

This strategic approach requires priority attention and a committed alliance of Canadian law enforcement agencies. Canada will need to look at maximizing the efficiencies of existing resources in order to ensure a more effective response in the continued effort to combat cyber crime both domestically and internationally. As technology evolves, so too must law enforcement's capabilities, training, labs and tools.

Adopting a collaborative approach Law Enforcement Agencies across Canada will deploy this strategy to effectively disrupt Cybercrime in their respective jurisdiction, and enhance Canada's reputation as a safe and secure nation within the global community.

### *Media Lines*

- Cybercrime has become an issue of national and international importance and significance that demands the attention of law enforcement agencies, intelligence agencies and the national/international justice system.
- The Dept. of Justice, via Bill C-30, is planning to ratify Canada's agreement to the Council of Europe's Convention on Cybercrime.
- Police services across the country are attending to the priority cases of cybercrime, often using a collaborative approach with partner agencies.
- Resources have yet to be secured to address a robust 24/7 capacity that would mimic the nature of cyber events.

- It is the recommendation of the CACP that all member agencies undertaking efforts to expand cybercrime programs and work with the RCMP Cybercrime Fusion Centre to develop an integrated strategy.

**WHEREAS** the problem of Cybercrime (i.e. criminal activity committed using a computer or targeting a computer) is causing significant concern in Canada, and;

**WHEREAS** the Canadian federal government, via Bill C-30, is planning to ratify the Council of Europe's Cybercrime Convention (aka Budapest Convention), and;

**WHEREAS** Cybercrime has emerged as persistent criminal activity in Canada, causing severe harm to the confidence of Canadians in their public safety, the resilience of the critical infrastructure systems they depend on and the integrity of their online identities;

**WHEREAS** Cybercrime erodes consumer confidence in the marketplace, directs harm at legitimate business, endangers consumer privacy and impacts the growth of our digital economy, and;

**WHEREAS** the ability of government and law enforcement officials to prevent, disrupt, or respond decisively to the evolving threat of cybercrime, is considered one of the most challenging priorities facing the policing of our nation today, and;

**WHEREAS** a strategic approach to cybercrime will compliment the work already undertaken via Resolution #09-2006 for a Mass Marketing Fraud Strategy, and;

**WHEREAS** there is a need for a coordinated and collaborative national strategy to disrupt, prevent and reduce the harm resulting from cybercrime and to apprehend, and prosecute, Canadian-based operators.

**THEREFORE BE IT RESOLVED** that the Canadian Association of Chiefs of Police calls upon the Government of Canada, together with its provincial and territorial partners through the federal-provincial, territorial process, law enforcement, the private sector and other partners to:

Support the requirement for a National Cybercrime Strategy to disrupt and neutralize Canadian-based cybercrime, through means centered around:

- The development of interagency capacity for increased coordination and collaboration;
- The identification of interprovincial and international operational plans to increase the effectiveness of law enforcement initiatives;

A national harmonized data collection point for Cybercrime complaints / incidents. This could include the existing Canadian Anti-fraud Centre (CAFC) as a strategic partner in this endeavour;

# Activities Planned/Significant Dates 2011/2012 :

| | |
|---|---|
| Fall  2011 | Committee Meeting<br>Québec City, Québec - October 6/7, 2011 |
| Spring 2012 | Committee Teleconference Meeting<br>April 4, 2012 |
| Spring 2012 | Committee Meeting<br>Edmonton, Alberta – May 2-4, 2012 |
| Summer 2012 | Annual CACP (No E-Crime Meeting scheduled)<br>(Sydney. Nova Scotia) |

- Establishing a recommended scientific methodology for the search, seizure and analysis of digital evidence

- Examine the requirement for the validation of technical tools and utilities

- Assess online training opportunities to reduce prohibitive training costs.

- Assess impact of Cloud computing in the scientific/forensic process and its foreseeable impact on court disclosure (reliability of seized data).

- Assess impact on encryption on forensic examinations and due process.

- Broaden committee membership (Lacking Eastern Canada representation).

- Identify opportunities for prevention and awareness

# COMMITTEE MEMBERS LIST:

**A.R. (Tony) Pickett**
Superintendent
OIC - Technological Crime Branch
RCMP Technical Operations
1426 St. Joseph Blvd.
Ottawa, ON
K1A 0R2
Telephone: (613) 949-8905
Fax: (613) 993-2963
Email: tony.pickett@rcmp-grc.gc.ca

Bio: Supt. Tony Pickett serves as the Officer in Charge of the Technological Crime Branch within Technical Operations and leads the RCMP's national Technological Crime Program. The program aims to improve the RCMP's investigative response capability on pure computer crime investigations and provide specialized technical investigative services including the search, seizure and analysis of digital and electronic evidence. It also produces and delivers investigative tools and utilities for technological crime operations through research, development, and validation. He is responsible for the development of national policy, provide program management services, and develop mitigation strategies through research, identification, and analysis of criminal trends in use of technology in partnership with domestic and international partners.

Supt. Pickett has over 25 years experience with the RCMP having served in various capacities. He joined the RCMP in 1985, after graduating from Memorial University of Newfoundland with a Bachelor of Arts. He began his career performing general duty policing in British Columbia. In 1989, upon being transferred to the RCMP National HQ, he served as both a Policy Analyst and Intelligence Officer in the Immigration & Passport Program. During his tenure within this Program, he represented the RCMP on various national and international working groups. In 2003, he was appointed the RCMP's National Public Security and Anti-Terrorism coordinator. This funding was a Government of Canada initiative to increase security after the tragic events of September 11th, 2001. It supported many initiatives including the creation of the Integrated Border Enforcement Teams and Integrated National Security Enforcement Teams. In 2006, he was assigned to Human Resources Sector and was promoted to Superintendent in 2007. From January 2008, until his current posting he provided strategic and management support services to the Deputy Commissioner Policing Support Services.

Supt. Pickett currently represents Canada at the Strategic Alliance Cyber Crime Working Group and the G8 Roma/Lyon Group - High Technology Crime Sub-Group. He is also the Co-Chair of the E-Crimes Sub-Committee of the Canadian Association Chiefs of Police.

**Martin Charette**

Lieutenant
Chief of Division
Technological Crime Support Division
Electronic and Informatics Surveillance Service
Sûreté du Québec
1701 Parthenais Street
Montreal, PQ
H2K 3S7
Telephone: (514) 598-4098
Fax: (514) 596-3096
Email: martin.charette@surete.qc.ca

Bio: Lieutenant Charette joined the SQ in 1989 and was assigned as a regional investigator in 1993. He was appointed in 1996 to the arson and explosives section as a major crime investigator in Montreal. He is an experienced investigator dealing with serious and organized crime.

In 2001, he was promoted to Staff Sergeant of a regional investigative unit. Lieutenant Charette assumed duties as the Officer in Charge for a regional detachment in 2004 before being assigned in charge of the electronic surveillance section of La Sûreté in 2005. He was reassigned to the Technological crime support division in 2007 in the same capacity. His responsibilities include overseeing specialists in Quebec City and Montreal as well as ensuring the support for all law enforcement agencies in the Province of Quebec. In 2010, a cyber surveillance team was integrated to provide a sole point of service for all technological assistance within La Sûreté's provincial mandate.

Lieutenant Charette was a member of the LAES (Lawful Access Electronic Surveillance) subcommittee of the CACP from 2005 to 2009. He has been a member the National Technological Crime Advisory Committee (NTCAC) since 2008 and of the E-Crime Committee since 2009. In 2010, Lt Charette accepted Co-Chair duties of the E-Crime Committee of the Canadian Association of Chiefs of Police.

**John Bilinski**

Superintendent
OIC – Canadian Police Centre for Missing & Exploited Children
RCMP Technical Operations
890 Taylor Creek Drive
Ottawa, ON
K1A 0R2
Telephone: (613) 841-0308
Fax: (613) 841-0553
Email: john.bilinski@rcmp-grc.gc.ca

Bio: Supt. Bilinski joined the RCMP in 1976 and has spent his career in a number of locations in Canada and overseas. He has in excess of 10 years of experience on the Montreal Drug Section as an investigator and undercover operator. He was transferred to Ottawa in 1988, where he worked in the National Drug Enforcement Branch coordinating investigations and training police officers. He was then transferred to Calgary, Alberta where he worked as a senior investigator on an integrated proceeds of crime section.

In 1996, Supt Bilinski participated in a United Nations Mission in Haiti training Senior Haitian National Police Officers. He was posted at the Haitian National Police Training Academy in Port au Prince, where he delivered a police Management Program designed to teach the principles of providing police leadership. In 1998, he was transferred to Edmonton Alberta as the Operations NCO in the Edmonton Integrated Proceeds of Crime Section. In 2000, he was transferred to Madrid, Spain where he worked as the Liaison Officer responsible for the effective exchange of police assistance in the Iberian Peninsula and seven countries in North Africa.

He was commissioned to the rank of Inspector and returned to Canada in 2004 where he headed the Commercial Crime Section in Edmonton Alberta. In 2007, Inspector Bilinski was transferred to the Canadian Police College in Ottawa where he was responsible for the Investigative Training program. In 2008, he was promoted to Superintendent and assumed the duties of Officer in Charge of the Canadian Police Center for Missing and Exploited Children.

## Ken MacKay

Superintendent
Edmonton Police Service
9620-103 A Avenue
Edmonton, AB
T5H 0H7
Telephone: (780) 421-2720
E-mail: Ken.Mackay@edmontonpolice.ca

Superintendent Ken MacKay joined the Edmonton Police Service in April 1979. He has held progressively responsible positions within the Service, serving in Patrol, Expert Collision Investigations, Tactical Section and Criminal Investigations. As an Inspector, Ken was assigned to Patrol and Corporate Planning Branch before being promoted to Superintendent in the Office of the Chief of Police. Ken is currently in charge of the Specialized Investigations Division.

Superintendent MacKay has a Bachelor of Physical Education and a Masters of Business Administration as well as numerous certificates and other advanced courses. Superintendent MacKay holds a number of professional affiliations and represents the Edmonton Police Service on international, national and local committees.

## Thomas Fitzgerald

Superintendent
Unit Commander, Intelligence Services
Toronto Police Service
40 College Street
Toronto, Ontario
M5G 2J3
Telephone: (416) 808-3513
Fax: (416) 808-3502
E-mail: thomas.fitzgerald@torontopolice.on.ca

Bio: Tom joined the Toronto Police Service as a Constable in 1980 after obtaining a Bachelor of Science Degree from York University.

Tom has a diverse skill set and has worked in the following areas of the Toronto Police Service: 53 Division, 55 Division 42 Division, 54 Division, Homicide Squad, Fraud Squad, Professional Standards, and is currently the Unit Commander of Intelligence Services. The vast majority of his service has been dedicated to investigative roles within these Units.

**Ian Kingham**

Inspector,
Investigative Support
Criminal Investigations Directorate,
Ottawa Police Service
474 Elgin Street,
Ottawa, Ontario
K2P 2J6
Telephone: (613) 236-1222 Ext: 5416
Fax: (613) 760-8122
Email: kinghami@ottawapolice.ca

Bio: Inspector Kingham has been a member of the Ottawa Police Service since 1986 and is presently the Officer in charge of the Investigative Support Division within the Criminal Investigations Directorate. The Units in this portfolio include; High Risk Offender Management (Mental Health Unit, Missing Persons, Dangerous Offenders/Long Term Offenders, Sex Offender Registry, High Risk/Repeat Offenders) Forensic Unit (Forensic Identification Section, Imaging Services, High Tech Crimes), Special Services (Surveillance and Air Support) and Property and Enterprise Crime (Organized Fraud, Elder Abuse, Organized Auto Theft, Arson)

Prior to his current role Inspector Kingham has been assigned to a number of areas of the police service in a variety of roles and ranks, including, Patrol, Forensic Identification, Fleet Management, Communications/911 Management, District Operations and District Investigations.

In 2002 Inspector Kingham worked with the RCMP and Vancouver Police in Port Coquitlam B.C. on forensics in the Willie Picton serial killing investigation under the Missing Women's Task Force umbrella. Inspector Kingham was also the co-creator of the Scenes of Crime Officer (S.O.C.O.) program for the Ottawa Police Service and served as one of the founding members of the original Chemical Biological Radiological Nuclear (C.B.R.N.) Team. The timing of the creation of the Ottawa Police CBRN team with the outbreak of "white powder" calls in a post 9-11 world put this team at the leading edge of these investigations from an evidence gathering and mitigation point of view. In 2010 Inspector Kingham completed his Bachelor of Policing degree through Charles Sturt University in Australia.

## Grant Foster

Superintendent
Saskatoon Police Service
P.O. Box 1728
Saskatoon, SK.
S7K 3R6
Telephone: (306) 975-8343
Email: Grant.Foster@Police.Saskatoon.Sk.CA

Superintendent Grant Foster has been a member of the Saskatoon Police Service for 33 years. After graduation from the Saskatchewan Police College in 1977, he was assigned to Patrol and also worked as a Constable in Communications Section, Special Investigation Unit (SIU) and Planning and Research Section. Superintendent Foster was promoted to Sergeant in 1998 and assigned to Fraud. In 2002, Superintendent Foster was promoted to Staff Sergeant and worked in Professional Standards.

In 2003, Superintendent Foster was promoted to Inspector and was Officer i/c of Records Management Division, responsible for Communications, Detention, Central Records and court operations transferring later in the year to Officer i/c Community Services Division. In 2004, he was assigned as the Acting Superintendent i/c Patrol where he remained until 2008 being promoted to the rank of Superintendent in 2006. In 2008, Superintendent Foster was assigned Detective Superintendent i/c Criminal Investigations.

Superintendent Foster has a two-year diploma from the Northern Alberta Institute of Technology, Edmonton, AB, an undergraduate degree from the University of Alberta, Edmonton, AB and a graduate degree from the University of Saskatchewan, Saskatoon, SK. He has attended several operational and administrative courses at the Saskatchewan Police College, Canadian Police College, RCMP Depot, Boston University and National Tactical Officers Association (NTOA). Superintendent Foster represents the Saskatoon Police Service on a number of committees and is currently the vice president of the Saskatoon Executive Officers Association.

Ray Archer
Canadian Bankers Association
888 Birchmount Rd., 6th Floor
Scarborough, ON.
M1K 5L1
Telephone: (416)-615-4557
Fax: (416) 615-5178
Cell: (416) 371-5845
Email: ray.archer@scotiabank.com

CANADIAN BANKERS ASSOCIATION
ASSOCIATION DES BANQUIERS CANADIENS

*Building a Better Understanding / Pour mieux se comprendre*

Bio: Ray is the Vice President & Deputy CISO of Information Security & Control at Scotiabank. His global responsibilities include: Security Operation Services (Change Control & UserID Administration), Vulnerability Management (Server & Desktop Security), Cryptographic Services, Technical Security Services (Network Security Center) and Security Intelligence and Forensic Services. Ray's previous post with Scotiabank was the Director of Technological Crime and Forensics - Corporate Security at Scotiabank. Between his careers with the Royal Canadian Mounted Police (RCMP) and Scotiabank he has gained over 31 years of investigational, technical and audit experience in the areas of criminal investigations, information technology and electronic data processing auditing. He has extensive experience in computer forensics, information security systems analysis, and provides a consultative role as an IT security specialist to all areas within the Scotiabank Group.

Ray joined Scotiabank in 1998 after serving 23 years with the RCMP. IT investigative and forensics experience was gained by various assignments, duties and formal education over the past 28 years. As a member of the RCMP - Security Evaluation and Inspection Team (SEIT), he performed IT audits on Federal Government departments processing highly sensitive information, as well as, providing a consultative role as an IT security specialist. Ray received a B.A. Degree from University of Manitoba and holds the Certified Risk Professional (CRP) and Certified Information Systems Security Professional (CISSP) designations. Ray is a member of the Computer Security Institute and is a security advisor to the Bank Administration Institute (BAI).

# ASSOCIATE MEMBERS

**John Weigelt**
National Technology Officer
Microsoft Canada
Ottawa, ON
Telephone: (613) 940-3337
Cell: (613) 298-4894
Email: john.weigelt@microsoft.com

Bio; John Weigelt is the National Technology Officer for Microsoft Canada. In his role, John is the lead public advocate on all aspects of Microsoft Canada's technology strategy as it relates to the development of national technology policy and the implementation and use of technology across the public and private sectors.

John previously held the role of Chief Security Advisor and Privacy Compliance Officer for Microsoft Canada. He was responsible or the development and communication of Microsoft Canada's security and privacy strategies for the organizations within the private and public sector and was instrumental in the development of a world leading partnership with the Canadian government.

Prior to joining Microsoft, John held the position of Senior Director of Architecture, Standards and Engineering at the Chief Information Officer Branch of the Treasury Board of Canada Secretariat. In this role he was responsible for the development of the Government of Canada Enterprise architecture, Treasury Board IM and IT standards and provides support for Critical Information Infrastructure Protection Policy.

John holds a Master's Degree in computer and communications security from the Royal Military College of Canada is both a certified information systems security professional as well as a certified information security manager.

**Bessie Pang**

Executive Director
The Society for the Policing Of Cyberspace (POLCYB)
Suite 480 - 2755 Lougheed Highway,
Port Coquitlam, B.C.,
V3B 5Y9
Telephone: (604) 927-1962
Fax: (604) 927-1955
Email: polcyb@telus.net

Bio: Bessie is a Criminology Consultant. Ms. Pang moved to Canada from the United Kingdom after receiving her B.A. Hons. in “Developmental Psychology with Cognitive Studies”, which focused on Psychology and Artificial Intelligence programming. After completing her M.A. Degree in Criminology in Vancouver, Bessie has been working in various fields of Criminology. While working at the BC Forensics Psychiatric Commission in Vancouver and the National Headquarters of Correctional Services Canada in Ottawa, Bessie specialized and published research in profiling risks/needs of juvenile and adult sex offenders, women offenders, and dangerous offenders.

Since returning to Vancouver from Ottawa, Bessie established Primexcel Enterprises Inc. to conduct Criminology and other business consultations. Ms. Pang was commissioned by the B.C. Forensic Psychiatric Commission to develop the first comprehensive “Standards and Guidelines for the, Assessment, Treatment and Management of Sex Offenders in B.C.” Bessie also has extensive experience in policy development; development of provincial and federal standards, including staff training and equity employment; program development and evaluations – including programs for youth gangs, community policing, and domestic violence.

Bessie is one of the founders of The Society for the Policing of Cyberspace (POLCYB) – an International Society based in Vancouver, B.C. Currently, in addition to other consultation projects, Bessie also is assuming the role of the Executive Director of POLCYB.

# TECHNICAL ADVISORS

Canadian Police
College
Collège canadien
de police

**France Thibodeau**
Manager, Technological Crime Learning Institute
Canadian Police College
P.O. Box 8900
Ottawa, Ontario
K1G 3J2
Telephone: (613) 990-2480
Fax: (613) 990-9738
Email: fthibode@cpc.gc.ca

Bio: France Thibodeau is a civilian member of the Royal Canadian Mounted Police. She has been the Manager of the Technological Crime Learning Institute at the Canadian Police College for more than ten years.

Ms. Thibodeau leads a team of eleven high-tech crime specialists consisting of RCMP Police officers and civilian members. Her team has trained thousands of police officers from across the Canada and countries from around the globe.

Ms. Thibodeau has a Bachelor of Science degree in Computer Science from the University of New Brunswick. Over the past decade, she has devoted significant time and effort to continuous learning in order to stay current in the fields of computer forensics, on-line investigative techniques, and in the latest adult learning techniques.

**Dan MacRury**

Senior Crown Attorney
Public Prosecution Service
Government of Nova Scotia
Maritime Centre
Suite 1325
1505 Barrington Street
Halifax, NS
B3J 3K5
Telephone: (902) 424-8734
Fax: (902) 424-0659
Email: macrurda@gov.ns.ca

Bio: Mr. MacRury, a native of Sydney, Nova Scotia joined Nova Scotia Legal Aid in 1989 and before that was in private practice. He was admitted to the bar in 1986. He is a graduate of St. Francis Xavier University in Antigonish and the University of New Brunswick Law School in Fredericton. Mr. MacRury was appointed as Crown Attorney in 1996 assuming responsibilities in the Cape Breton Region. Mr. MacRury was transferred to Halifax in 1998 where he continues to practice today.

Mr. MacRury is a member of the Federal/Provincial/Territorial Working Group on Cyber crime and is well versed in the complex legal issues that have arisen since digital evidence has been introduced into the judicial system. Mr. MacRury is the Vice-President of the Canadian Criminal Justice Association.

Department of Justice Canada Ministère de la Justice Canada

**Gareth Sansom**

Director, Technology and Analysis
Lawful Access Group,
Criminal Law Policy Section
Department of Justice Canada,
284 Wellington Street, EMB 2061,
Ottawa, ON,
K1A 0H8
Email: GSansom@JUSTICE.GC.CA

Bio: Gareth has been a policy advisor in the Canadian federal government since 1990. His work has always dealt with advanced communications networks, often involving public safety questions, in the context of which he has conducted research on the issues of obscenity and child pornography online. Gareth was the author of Industry Canada's public discussion paper *Illegal and Offensive Content on the Information Highway* (released June 1995), which was one of the first public Canadian government documents to deal with the question of child pornography and obscene material on the Internet. Prior to joining the Department of Justice Gareth was with the Electronic Commerce Task Force at Industry Canada where he was senior advisor in cryptography policy.

In 2001, Mr. Sansom received a Recognition Award from the Deputy Minister of Justice in acknowledgment for "exceptional dedication and extraordinary efforts in developing the Government of Canada's policy and legislative proposals to respond to the decision of the Supreme Court of Canada in the case of *Regina v. Sharpe* (2001)", a case challenging the constitutionality of Canada's *Criminal Code* provisions regarding the possession of child pornography.

Gareth received his B.A. Honours from Trent University and an M.A. in Communications from McGill University where he also undertook doctoral studies. Gareth has taught a variety of university courses in Mass Communications at Carleton University including courses on post-industrial society and information security.

Gareth's current work with the federal Department of Justice is focused on high-tech crime issues including child pornography on the Internet, as well as the technical and legal aspects of lawfully authorized electronic surveillance.

**Alex Smith**

Ontario

Ministry of the
Attorney General

Director, Law and Technology
Crown Law Office – Criminal (Ont.)
9th Floor, 720 Bay Street,
Toronto, Ontario
M5G 2K1
Telephone: (416) 212-1166
Email: alexander.smith@jus.gov.on.ca

Bio: Alex Smith (B.A., M.A., L.L.B.) is currently the Director of Law and Technology for the Ministry of the Attorney General, Criminal Law Division. Upon graduating from the University of Windsor Law School in 1981, Alex was named to the Dean's Honour Roll, and was the recipient of the CCH Prize for Legal Writing. Alex completed his Articles at the Office of the Crown Attorney in London. Following his call to the Bar in 1983, he was hired as an Assistant Crown Attorney in Lindsay. In 1986 he transferred to the Brampton Crown's Office and in 1989 joined the Guelph Crown Attorney's Office where he remained until 2001, at which time he was appointed to his current position.

In his current position, Alex manages information technology issues for the Criminal Law Division. He Chairs the Attorney General's Task Force on Internet Crimes Against Children and the Division's e-Disclosure Committee and participates in a number of other committees at the provincial and federal levels. Alex has organized and participated in numerous educational programs as a panelist or lecturer and is a frequent speaker at continuing legal education programs. In addition to the responsibilities associated with his current position, Alex continues to represent the Crown at all levels of trial and appeal courts.

**Marc Moreau**

Staff Sergeant
Technological Crime Branch
Strategic Communications & Liaison Officer
1426 St-Joseph Blvd.,
Ottawa, ON K1A 0R2
Telephone: (613) 993-6011
Fax: (613) 993-2963
Email: marc.moreau@rcmp-grc.gc.ca

Bio: S/Sgt Moreau is a member of the Royal Canadian Mounted Police with 32 years of service. He is currently in charge of Strategic Communications & Liaison Officer for the National Technological Crime Program.

S/Sgt Moreau has been engaged in technological crime field since 1992, having served in various capacities within the Tech Crime Program. Following several years of conducting technological crime investigations, S/Sgt Moreau pursued his interest in this field by joining the Canadian Police College as an instructor at the Technological Crime Learning Institute in 1997. This afforded S/Sgt Moreau with the opportunity to provide the specialized training to the various police agencies across Canada as well as international police services engaged in technological crimes.

In 2002, S/Sgt Moreau joined the Technological Crime Branch to assume managerial duties in the service delivery of the Program. S/Sgt Moreau was responsible for the implementation of the Understudy Program in 2003. This level of standard was shared with other law enforcement agencies domestically and internationally. This was also a model that was accepted in 2009, as a national standard for Canadian law enforcement agencies. He supervises the development of national program policies and service standards which impacts the operations of the Technological Crime Program in Canada which includes overseeing the field Units located in the major centres across Canada.

S/Sgt Moreau is responsible for developing, directing and delivering strategic internal and external communications programs to support the advancement of the RCMP Tech Crime Program business objectives. He also provides advice to national/international stakeholder partners regarding cyber crime issues and its potential impact on law enforcement in Canada and abroad.

# Appendix "A"

## Minutes of NTCAC & CACP E-Crime Committee Meeting

**October 5/7, 2011**
**Quebec City, Quebec**

**Participating:**

| | |
|---|---|
| Tony Pickett (E-Crime Co-Chair) | RCMP – Ottawa |
| Martin Charrette (E-Crime Co-Chair) | Sûreté du Québec |
| Francesco Secondi | Service de police de la ville de Montréal (SPVM) |
| Louis Jacob | Sûreté du Québec |
| Il Kim | Sûreté du Québec |
| Francesco Secondi | Montréal SPVM |
| Jeff Mitchell | Peel Regional Police Service |
| Kevin Mallay | RCMP Nova Scotia |
| Jean-Francois Bernier | Quebec City Police Service |
| Danny Smyth | Winnipeg PS |
| Kevin Riel | Winnipeg PS |
| Grant Foster | Saskatoon Police Service |
| Paul Batista | Ottawa Police Service |
| Bill Bosward | Toronto Police Service |
| John Menard | Toronto Police Service |
| Joel Bautista | Saskatchewan ICE Unit |
| Craig Coughlan (Chair NTCAC) | Calgary Police Service |
| Dale Heinzig | Calgary Police |
| Phil Palamattam | Edmonton Police Service |
| Gareth Samson | Justice of Canada, Criminal Law Policy |
| France Thibodeau | Canadian Police College |
| Carole Matthews | OPP - Orillia |
| Marc Moreau | RCMP – Ottawa |

**Regrets**:

| | |
|---|---|
| Tom Fitzgerald | Toronto Police Service |
| Grant Foster | Saskatoon Police Service |
| Ray Archer | Canadian Bankers Association – Ontario |
| Ken MacKay | Edmonton Police Service |
| Bessie Pang | Society for the Policing of Cyberspace |
| John Weigelt | Microsoft Canada |
| Alexander Smith | Attorney General, Crown Law Office – Ontario |
| Dan MacRury | Nova Scotia – Public Prosecution Service |

**Day 1 NTCAC Wednesday October 5th, 2011**

**Opening Remarks**

Roundtable.

Overview of committee goals. NTCAC was created in 2008. Provide input to CACP e-Crime Committee.

**Review of Old Business**

Tenure

- NTCAC recommends tenure of a minimum of 5 years for tech crime analysts.
- Also recommends following the two year understudy program.
- Statement on tenure position submitted to CACP e-crime committee.

Use of Civilians

- Overview of document
- NTCAC recommends police officers be used as forensic analysts, however does identify that some agencies have adopted the hybrid model.
- Cited need for knowledge of criminal offences and investigative knowledge and experience
- Bottom line is that the analyst is still conducting a police investigation.
- Issues raised which may require further discussion include:
  - Clothing and equipment
  - Special constable status
  - Retention and pay

- Use of civilian as full analyst vs. support position
- Naming in warrant, attending searches
- Clear sop's on tasks/assignments
- Communications between civilians and requestor (the case investigator)

Understudy Program

- Mark Moreau indicates that the understudy program developed by the NTCAC has been shared with Germany. All members of the group should be proud that Canada has one of the only National Understudy Programs of this nature.

Encrypted SD cards in blackberries

- Craig discusses issue.
- Member had blackberry stolen – question arises how secure was the encrypted SD card?
- If you encrypt your bb with a password and you have an SD card – by using software you can acquire the password on the SD card which will be the same password as on the handset.
- Elcomsoft is the company (Russian) specializing in system security and password recovery. Software was $400 (this was not the whole bundle)
- Only works on the newest version of bb's. Works on Torches and 9000 series.
- Company also makes a software to crack IPD files (lots of people use the same password when they back-up their bb on their computer)

**New Business**

Management of Tech Crime Units

Phil provides over view of his unit (Edmonton Police Service)

- Processes for discussion: RFS, Priority Assessment, Case Management and Reporting, Retention
- Have an electronic RFS form – review of a copy of their form
- RFS includes a scaled (drop down windows) that provides a "rank" for the request. This assists with prioritizing the RFS.
- Information is then moved to the case management system. Use an open source application called "trac". Program is used for forensic analysis.
- Creates a "ticket", program has all information from the RFS including the rank.
- Allows for attachments.
- Monitors court dates, issues that affect resources, tracks communications between members

- Also use “wiki” – administration, infrastructure and knowledge base TCU application.

Craig provides overview of his unit (Calgary PS)

- IT equipment – don’t go through IT, they purchase, but the regular approval process doesn’t have to be undertaken.

Martin Charette

- Full forensic analysis (tech crime) – most of resources are computer examination and data extraction.
- Also conduct Cyber Security investigations (IP look ups etc)
- Also have a component for internet intercepts – tie into the lawful access side to support investigative units
- Co-located with Quebec City and Montreal City
- Also have civilian support (network support) and an engineer (programming)

Winnipeg

- Tech Crime unit under forensic services
- 7 detectives and 2 Detective Sergeants
- Dedicated ICE investigators
- Good working relationship with RCMP
- Technical support unit
- Tech crime merged from commercial crime
- Units tend to be stand-alone, managed under support unit

RCMP

- 13 field offices across the country

Quebec City

- 3 members – have worked in partnership for the last three years with SQ and RCMP

RCMP Nova Scotia

- H Division – falls under DIO (Division Intelligence Officer), however work closely with ICE
- One fulltime civilian member
- 3 full time uniform members
- Could easily be double
- Have backlog, 104 cell phones waiting for analysis (60 files), 40 computers (25 files)
- At stage that they need to implement a prioritization model
- Have developed a software package to help with cue times etc.
- Forensic methodology – have a document that outlines their methodology

Peel Regional Police

- Reports to Sexual Assault Unit (no connection to the Unit)
- Believes the best fit would be under forensic identification
- They don't have a nexus with Intel
- 7 constables and one full-time civilian
- IT is separate from the corporate IT
- 150-200 devices (80-100 occurrences)
- Need to look at a system of prioritization – need criteria and concrete scoring so it's more consistent

Montreal PS

- Co-locate with SQ
- Stand alone unit
- 5 forensic officers
- 1 officer – used for compliance/training, new members spend first 6 months with him,
- 3 investigators – support all other investigative units (IP tracking, warrants, anything to do with virtual investigations)
- 2 civilian technologists
- Separate IT network
- Last year 700 files, this year 2200 files
- Backlog is at about 41 weeks
- Have put in a demand for 8 new people (will probably be internal)
- Thinking of creating new division – incorporate supertext, Ident etc..

Ottawa

- Evolved out of funding from province for ICE.
- Started with RCMP, DND and Ottawa PS doing all aspects of ICE from investigation to forensics.
- Received money from the province which started the program.  Didn't get much attention in the beginning.  Off-site and dysfunctional – moved to Criminal Investigations
- 4 ICE investigators and 1 Sgt (3 year tenure)
- 4 forensic investigators (5 year tenure), one new Sgt coming (or perhaps an investigator)
- Within last 18 months – ICE went to sex assault side, forensic investigators went to Forensic Ident side
- After separation from RCMP – issues are equipment purchase.
- Problem – not a lot of people apply for positions (hard to get a pool of candidates).  Also have tenure, which is a problem in the forensic area.
- Funded by the province through the Provincial Strategy

Saskatoon

- 2009 – proposal for a provincial strategy – fell under Vice.
- Minimum 8 years experience before applying to tech position
- ICE – RCMP and three municipal Police Services
- Total 12 members and 1 staff sergeant
- Saskatoon – has Tech area, ICE falls under a different area which is mostly provincial funding
- Tenure: 3-5 years
- Use Saskatoon file management system, outside of this, RCMP prose file. Joel uses a spreadsheet to track cases.
- Backlog is about 3 months (Joel has 25 occurrences)
- Expansion and new building being built. ICE will meld with Tech area.

**Similar Issues Identified:**

- Development of investigative units with no consideration for back-end technical support (tech crime)
- Lead to increased back-logs, lead to field or investigative units trying to adopt forensic practices (want to do it themselves so it gets done), no training, no forensic skills etc..
- Need for system of prioritization/ranking cases (electronic case management system). Development of a ranking tool/case management program.

**Craig Coughlan – Provides overview of scoring criteria to rank requests for service**

- Categories: Type of Occurrence, Evidentiary Value to Case, Focus of Search, Requesting Unit (internal vs. external agency request), Urgency, Days to Court, Other Factors
- Create File Intake Matrix – each case gets a total score based on values assigned.
- Low scoring file gets 4 additional points for every month that elapses
- Standard e-mails to remind investigators about the status of open cases (yearly)

**Forensic Utility Research Team (FURT) presentation**

Provides technical forensic research and development tools
LANA Project – Low Attribution Network Access Project. Taliesin system. Used to overtly access the Internet for open source data mining with near total anonymity. Covert browser. Why? To avoid being identified as a government or law enforcement official.
Jocelyne Beachamp-Brule. Manager Forensic Utility Reasearch Team, Tech Crime Branch, RCMP, 616-991-1315, e-mail: jocelyne.brule@rcmp-grc.gc.ca

Apparently Microsoft has developed a similar type system.

**Lawful Access Legislation**

The group is looking for actual examples of stats you have about these requests. Or anecdotes. Have to be disclosable.

Trying to pass legislation that the service provider has to provide subscriber information without a warrant. There will be a time limit attached to the response

**Round Table**

Looking for input on what our topics should be for the next year.

- Martin encourages members to review CACP report. Might be nice for NTCAC to bring forward proposals/issues that should be brought to the attention of the CACP.
- Disclosure. What should be included in a disclosure report. Issues are the vast amount of data now stored on devices. Impossible to disclose everything now.
- Defense using IT specialists to bring disrepute on investigators.
- Virtual Machines.
- Scope of the Warrant. Secondary warrants.
- Encryption. Encrypted hard drives, volumes of encrypted drives, encrypted files. No laws to assist.
- Cloud computing. Seizing data in its whole entirety. Impact of storage capacity issues.
- Storage/Data Retention: storage of evidence on back-ups. What do we have to store. What can we eliminate EO1 files, how long does everyone store the data? Retention rules. Best practices in relation to authority to retain, how long, etc. What is considered an “original exhibit”. In some instances, we may not even have authority to retain information. If the original evidence is ordered returned or destroyed.
- Discuss/share prioritization schemes (ranking)
- Overview of state of Tech Crime Units/Report: backlogs, staffing, issue of staffing other investigative units with no forethought to impact on tech crime units, Lead to increased back-logs, lead to field or investigative units trying to adopt forensic practices (want to do it themselves so it gets done), no training, no forensic skills etc..

- Need for system of prioritization/ranking cases (electronic case management system). Development of a ranking tool/case management program.

- Gareth: Analysis on expectation of privacy – IP addresses have a low expectation of privacy. Whether there will be an expectation of privacy in relation to IP addresses is a huge concern. IPv 6[1] in 2012.

[1] **Internet Protocol version 6** (**IPv6**) is a version of the Internet Protocol (IP). It is designed to succeed the Internet Protocol version 4 (IPv4). The Internet operates by transferring data between hosts in small packets that are independently routed across networks as specified by an international communications protocol known as the Internet Protocol.

Each host or computer on the Internet requires an IP address in order to communicate. The growth of the Internet has created a need for more addresses than are possible with IPv4. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with this long-anticipated IPv4 address exhaustion, and is described in Internet standard document RFC 2460, published in December 1998.[1] Like IPv4, IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks. While IPv4 allows 32 bits for an Internet Protocol address, and can therefore support $2^{32}$ (4,294,967,296) addresses, IPv6 uses 128-bit addresses, so the new address space supports $2^{128}$ (approximately 340 undecillion or $3.4\times10^{38}$) addresses. This expansion allows for many more devices and users on the internet as well as extra flexibility in allocating addresses and efficiency for routing traffic. It also eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address autoconfiguration), network renumbering and router announcements when changing Internet connectivity providers. The IPv6 subnet size has been standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from link layer media addressing information (MAC address). Network security is also integrated into the design of the IPv6 architecture, and the IPv6 specification mandates support for IPsec as a fundamental interoperability requirement.

The last top level (/8) block of free IPv4 addresses was assigned in February 2011 by IANA to the 5 RIRs, although many free addresses still remain in most assigned blocks and each RIR will continue with standard policy until it is at its last /8. After that, only 1024 addresses (a /22) are made available from the RIR for each LIR – currently, only APNIC has already reached this stage.[2] While IPv6 is supported on all major operating systems in use in commercial, business, and home consumer environments,[3] IPv6 does not implement interoperability features with IPv4, and creates essentially a parallel, independent network. Exchanging traffic between the two networks requires special translator gateways, but modern computer operating systems implement dual-protocol software for transparent access to both networks

- Extraterritorial access to information (how do LEA's seized information that is stored in other countries) (based on Gareth's presentation for development of laws in relation to cyber security)

- Marc Moreau requires input on key messages so that when any agency takes media calls there is some standard wording

- From an international perspective, Marc Moreau would like to see at least 2 botnet investigations here in Canada (perhaps one national and one international)

**Action Items:**

1. Craig Coughlan to share scoring scheme.

2. Marc Moreau to share the presentation on the LANA Project.

3. The Lawful Access Group would like actual examples on stats, or anecdotes that your agency may have in relation to requests to service providers for subscriber information. Please remember this has to be disclosable. What situations to we need the information? Child porn, suicide etc.. (advise investigators that unless we get examples, the legislation won't go through and investigators will require warrants or production orders).

**Next Steps – Items for Discussion at Next Meeting:**

- Carole to present on eTracker at next meeting.

- How do Tech Units handle storage/data retention issues?

either natively or using a tunneling protocol such as 6to4, 6in4, or Teredo. In December 2010, despite marking its 12th anniversary as a Standards Track protocol, IPv6 was only in its infancy in terms of general worldwide deployment. A 2008 study[4] by Google Inc. indicated that penetration was still less than one percent of Internet-enabled hosts in any country at that time.

**Day 2 NTCAC Thursday October 6th, 2011**
**NTCAC jointed by CACP eCrime Committee Members**

**Presentation by Marc Moreau on the RCMP Cyber Crime Fusion Centre**

- Non operational entity – RCMP asked for 225 resources. Were awarded 5 with some funding to research and build a business case.
- October is Cyber Security Awareness month and the CCFC has been active in planning awareness. (website)
- CCFC has two deliverables:
    1. Annual report on Cybercrime in Canada (first report will be March 2012)
    2. A business case for new investigational capacity for law enforcement in Canada. Referred to as Cyber Crime Strategy. Best guess due date is when PS goes back to Cabinet with an update on the Cyber Security Strategy.
- Supt. Tony Pickett brings up some issues/concerns with gathering the information to support the business case (mandatory reporting legislation to report hacking, victimless crimes, business not reporting as they don’t want to tarnish their product, police capacity to respond to on-line crimes, order of magnitude – if crime is small in scale police may not investigate as opposed to larger scale/multi-jurisdictional investigations, non-reporting by victims). These things make it difficult to examine the scope of the problem. The dollar value reported by virus companies is large as compared to stats recorded by police.
- Empirical data seems to be missing. This is one of our challenges.
- Marc Moreau – indicates that NTCAC and CACP committee’s can help coordinate and provide stats for research.
- CACP would like to propose the need to support the Cyber Crime Strategy as a resolution.
- Looking for interested members to give CCFC advise or direction.
- Marc Moreau suggests that we have a teleconference in January 2012.

**Presentation by Philippe Gravelle and Sebastien Bourdon-Richard – Botnet Investigation**

- Complaint from major pharmacy chain in Québec that their gift card validation system had been compromised.
- Potential loss 2.2 million dollars (friend of suspect)
- Search warrant issued, located botnet control interface named Hwclient (seemed to be controlling computers)

- Suspect – encrypted all computers, used partitions on computer, second partition encrypted, had script to auto lock, computer at set time (noon).
- Discussion on "Live Forensics". Third search warrant, suspects computer was on, started a network capture to capture all network traffic. Use COFFEE RCMP Edition. Were able to obtain live memory capture.
- Everything was encrypted with TrueCrypt. Found password file in information from live forensic capture of live memory. Were then able to use passwords to access areas of the computer.
- Suspect had control of about 45 computers (victims)
- Located child pornography as well
- Suspect arrested and currently charged with 2 criminal offences
- Activity continues since release
- International implications?

Presentation by Gareth Sansom – Data stored outside of a country's borders

- Extraterritoriality – refers to the projection of a states jurisdiction beyond its own territory
- Involves the application of governmental authority to persons, places, and property located on the territory of their states or in other areas.
- Governing principles of international law with respect to extraterritoriality are: 1. respect for the territorial sovereignty of states 2. non-interference in the internal affairs of other States (respect for their independence) 3. the requirement of a real and substantial connection between the state
- Three kinds of jurisdictions 1. Prescriptive jurisdiction 2. Adjudicative jurisdiction 3. Enforcement jurisdiction
- Enforcement jurisdiction – the power to use coercive means to ensure that rules are followed
  - Enforcement jurisdiction is exclusive and geographically limited to the territory of each State
- Prescriptive jurisdiction: relates to the authority vested in the legislative bodies of State to make laws. (ie trade embargo on Cuba) by virtue of parliamentary sovereignty, parliament may enact legislation that violates international law, including in the are of extraterritoriality. (example child sex trade)
- Adjudicative jurisdiction: power of a state's courts to resolve disputes or interpret the law through decisions that carry binding force (Libman) for example it is possible to prosecute a person in Canada for criminal activities that have victims in another country if here is a real and substantial connection to Canada.

Various Mechanisms to Assist

- MLAT (common complaint – these mechanisms can be slow)
- International Treaties such as the Council of Europe Convention on Cybercrime
- Non-binding instruments (Commonwealth "Harare" Scheme)
- Possible new approaches to explore:
    - Memoranda of Understanding between states
    - Service provider contracts and subscriber agreements

Discussion around providing Gareth with suggestions on the requirements of law enforcement to access data that exists outside of a countries borders.

Marc suggests "MLAT" on steroids. Doesn't address the issue of "Live Analysis" (as a technique)

Gareth requires facts on the potential impact of access to information that exists outside of our country. This will assist him in negotiating at an International level.

**Next NTCAC meeting in Edmonton in May 2-4, 2012**

ARIN – next Wednesday vote on resolution 2011-7 (Compliance). Martin will forward the information.

**October 7th – CACP e-Crime Committee meeting**

Carole to coordinate review of mandate.
How do we develop and deliver our position on issues.
Building a cybercrime security strategy for Canada. What is the vision for Canada.

Mandate:

To establish a leadership role in the development of an administrative policy and standards for technology-based investigations, including the promotion of inter-agency cooperation in the prevention, detection and investigation of internet-based crime, the establishment of training standards, the identification of effective cooperation strategies to combat e-Crime at local, provincial, national and international level and to facilitate public education on information security.

Mandat :

Assurer un rôle de leadership dans l’élaboration d’une politique et des normes administratives relatives aux enquêtes technologiques, y compris la promotion de la collaboration interorganismes dans la prévention, la détection et les enquêtes relatives aux crimes sur Internet, à l’établissement de normes de formation et à la détermination de stratégies de coopération efficaces afin de lutter contre la cybercriminalité aux échelons local, provincial, national et international et de favoriser la sensibilisation du public à la sécurité de l’information.

Strategic Priorities/Objectives:

- To identify electronic crime investigation and prosecution issues to police leaders, to provide options for change and to exploit opportunities to enhance community safety
- To establish a leadership role in the development of administrative policy and standards for technology-based investigations
- To promote cooperation in the detection and investigation of computer-based crime

## Major Initiatives & Activities 2010/2011:

- Develop a standard forensic methodology for the search, seizure and analysis of digital evidence.
- Examine the requirement for the validation of technical tools and utilities.
- Analyze human resource challenges in specialized technical enforcement programs in relation to retention and tenure.
- Examine the role of civilian members/employees in specialized technical investigative services.
- Assess DVR (Digital Video Recorders) impact on law enforcement and explore solutions. NTCAC will assess the growing use of DVR for surveillance for public and commercial security.
- Broaden committee membership (lacking Eastern Canada representation).
- Monitor PIPEDA and its possible impact on law enforcement (following 5-year review).
- Monitor CIRA (Canadian Internet /ICANN – Internet Corporation of Assigned Names and Numbers) with regards to WHOIS policy.
- Identify opportunities for prevention and awareness.

## Principales initiatives et activités 2010-2011 :

- Développer une méthodologie en analyse de scènes de crime pour chercher, saisir et analyser les preuves numériques.
- Examiner la nécessité de valider les outils et services techniques.
- Analyser les défis des ressources humaines liés à la rétention et la durée dans les programmes spécialisés d'application technique.
- Examiner le rôle des membres civils et employés des services d'enquêtes techniques et spécialisés.
- Évaluer l'impact des enregistreurs vidéo numériques sur les corps policiers et explorer des solutions. Le comité consultatif national sur les crimes technologiques évaluera l'utilisation croissante des EVN dans la surveillance publique et commerciale.
- Élargir la composition du comité (l'Est du Canada n'y est pas représenté).
- Surveiller la LPRPDE et son impact éventuel sur le travail policier (à la lueur des cinq dernières années).
- Surveiller l'ACEI (Autorité canadienne pour les enregistrements Internet) quant à la politique touchant le bottin Internet.
- Identifier les occasions de prévention et sensibilisation

ARIN policy proposal 2011-7 Compliance Policy

- No enforcement/compliance to register IP addresses
- This policy is critical to law enforcement and Internet safety as it ensures ARIN IPv4 and IPv6 allocation and reassignment (recording in WHOIS) policies will be enforced. This policy proposal is to force compliance on IP address registration. There was too much opposition in the way the enforcement was presented.
- The resolution will be addressed at the next meeting (ARIN website). Will be an open discussion session followed by a vote. Wednesday Oct 12th at 2pm. Have to pre-register to vote on-line.

ICANN – Due Diligence

- ICANN governs the internet at an International level. Created in 2000.
- Bottoms up approach, hold public meetings
- Make recommendations to the Government Advisory Committee (GAC)
- LE assists by attending ICANN meetings and providing input.
- 2009 – put forward LE due diligence recommendations.
- Since 2010 – have met with the registrar community to get endorsement
- Due Diligence recommendations have support from many international organizations
- DD – telling registrars, “know who your customers are”. Some countries don’t care who their registrants are, they just want to make money.

ITU

5 registry’s in the world. ARIN is one. ITU has asked to become a registry (which they have not been allowed). ITU unlike ICANN has a top down approach.

IGF – internet governance board (developed by the UN). Pro developing countries, human rights driven.

**Encryption Survey and Pre-paid Cell Phone Survey – at the request of the FPT Working Group**

Discussion around partaking in survey. Apparently the Survey started being developed in Manitoba a few years ago. The survey has been re-worded several times. A review of the survey questions indicates the FPT group are looking to validate that there is a problem, when we know the problem already exists.

In 2007 – CACP put forward a resolution having to do with encryption. From a LE perspective we have already accepted that there is a problem. 2007-

Need re-focus – we are prepared to help, we want to get to the right type of survey.  Scrutiny will come to the stats once they are reviewed/used to make decisions in law.

There needs to be some evidence that there is an issue, which is based on actual statistics. However, how much information is required. Is there a threshold or just a need to justify the problem?

Gareth indicates that the scope of the resolution should be narrowed so that you can get to the specific resolution.  For encryption, should be clear that the problem is not the elimination of encryption because there is an obvious need for encryption of the the protection on information, you need to get to the specific issue that the need is to compel a suspect/accused to provide a password to compel evidence/testimony.  This eliminates the problem from getting too big. Constrain it to the type of offence/case/matter etc…

Carole to send out list of topics to Marc Moreau to rank top 5 issues to be addressed in the next year.

Review of mandate and strategic plan – for input to all members

G8 High Tech Crime Sub Group – Tony looking at some type of an international botnet investigation.

# Appendix “B”

CACP e-Crime Committee

**Teleconference of 2012-04-04**

**PARTICIPANTS**:

| | |
|---|---|
| Tony Pickett (Co-Chair) | RCMP, Ottawa |
| Martin Charette (Co-Chair) | Sûreté du Québec |
| Ken MacKay | Edmonton Police Service |
| Francesco Secondi | Service de police de la Ville de Montréal (SPVM) |
| Ian Kingham | Ottawa Police Service |
| Carole Matthews | OPP |
| Detective John Menard | Toronto Police Service |
| France Thibodeau | Canadian Police College |
| Gareth Sansom | DOJ |
| Ray Archer, | Canadian Bankers Association |
| John Weigelt | Microsoft |
| Marc Moreau | RCMP, Ottawa |

**REGRETS:**

| | |
|---|---|
| Grant Foster | Saskatoon Police Service |
| Mark Fleming | RCMP "E" Div |
| Ron Gentle | OPP |
| Tom Fitzgerald | Toronto Poilce Service |
| John Bilinski | RCMP. CPCMEC, Ottawa |
| Bessie Pang | Society for the Policing of Cyberspace |
| Dan MacRury | Nova Scotia - Public Prosecution Service |

**Summary of discussions**:

**Item #1: DOJ Questionnaire - Mr. Gareth Sansom, DOJ**

Mr. Sanasom advises that he has managed to get some of this work onto the work plan of the Quintet of Attorneys General, as a medium-term project. He would like for the NTCAC and E-Crime to review the questionnaire and provide comments, preferably prior to the Edmonton meeting.

It should be noted that Mr Sansom will also provide  briefings concerning his meetings in Washington with US DoJ and FBI.  He will also report on the United Nations International Experts Group dealing with Cybercrime, now that their questionnaire is being cicrculated

**Item # 2: National Cyber Crime Strategy - Mr. David Black, RCMP, Ottawa**

Cyber "Crime" Strategy: designed to compliment the Public Safety, Canada Cyber "Security" Strategy

- a two year project window, from now, to deliver a final version
- it may serve to address recommendations coming out of a forthcoming OAG report this fall
** This is not an RCMP-only solution. This is inclusive of the broader Canadian law enforcement community
- we count on the CACP executive (through the e-crime committee) to be a prime sponsor of the outcomes
- we depend on participation of some key CACP e-crime workgroup members
- this initiative will be the focus of the Resolution for the E-Crime Committee for this year. This is to reflect the fact that the Canadian LE community sees a need for such a strategy.

What are the implications for volunteers:

- much has already been written on this from the Council of Europe (COE), UK and Australia sources.
- we simply want to create a Canadian version
- our basic objective is to write the "costed business case" for new resources where needed.
- we anticipate the hire of a "strategy consultant" to reach out to industry stakeholders (for an unbiased perspective)
- we have just engaged another Sgt (Tim Cooke) to lead the writing here in the CCFT. He will engage well with our field Units across the country and would like to meet with you.

* The following (moderate) workload for those volunteering could include:
- we will meet with you individually - to consult for half day this summer

- we will have a group meet for half- in conjunction with a fall CACP E-crime workgroup meeting
- we will have another individual half day meet prior to any 2013-spring  E-crime workgroup meeting
- a final half day group meeting, prior to release of final draft.
- after each meet, there would be the normal exchange of emails to ensure we had captured points correctly
- volunteers will be responsible for briefing up to your senior executive as appropriate.  We anticipate writing some generic briefing points that could be used by all.

In summary, we do the writing around things you think are important to your agency - in line with other international strategic approaches already written.
Minimum effort would be a few days of email & document reviews and 2 days of meetings over two years.  At your address or in conjunction with CACP e-crime committee meetings.

Following discussions concerning the above the following police services volunteered to be part of the Working Group:
- Sûreté du Québec
- Ontario Provincial Police
- Calgary PS
- Montreal (SPVM)
- Ottawa PS
- Toronto PS

Thank you for those volunteering for this WG. Much appreciated. You can expect to be contacted by Mr. Dave Black soon.

**Item #3: Strategic Plan - Supt Tony Pickett, RCMP, Ottawa**

Advises this matter has been up for discussion in the past and we will need move forward in developing a new one. The current Strategic Plan was for 2009-2012. He mentioned that he would like the NTCAC to have this as an Agenda item for discussion at the upcoming meeting in Edmonton. This matter would be further discussed and hopefully finalized during the E-Crime Committee meeting. The goal is to have a new Strategic Plan by the end of our meeting in Edmonton.

## Item #4: Training Opportunities - S/Sgt Marc Moreau, RCMP, Ottawa

The RCMP Technological Crime Branch, National Policy Centre has been working with the Computer Emergency Team (CERT) from Pittsburgh, Pennsylvania to have some e-learning courses made available to the Canadian LE agencies. This is an initiative that we have been working on for the past few years. The progress has been hampered due to other priorities at CERT. However we have recently been informed that CERT has renewed their commitment to this initiative with a view to perhaps have these e-learning courses up and running by the Fall of 2012. We are aiming to bring this to fruition by the Fall meeting of the NTCAC/CACP, if not sooner. The cost for these courses have not yet been determined but it is expected they will be very reasonable.

In addition to the e-learning initiative (above) the CERT also has also developed a scenario based virtual exercise training modules that may be of interest to the Canadian law enforcement community. We expect to have a live demonstration of these capabilities at our upcoming NTCAC/E-Crime Committee meeting (Thursday - joint session day).

A further teleconference was held on Tuesday, April 10, 2012 between S/Sgt Craig Coughlan, S/Sgt Carole Matthews and S/Sgt Marc Moreau to discuss potential Agenda items for the upcoming meetings. Here were a few suggested ideas:

- Training, including an update from the Canadian Police College, Technological Crime Learning Institute
- Lawful Access update
- Presentation by the RCMP Integrated Technological Crime Unit (ITCU)
- Validation
- Search Warrants/Court Procedures
- Cloud computing
- ARIN update
- ICANN update

# Appendix "C"

## Minutes of NTCAC & CACP e-Crime Committee Meeting

**May 2-4, 2012**
**Edmonton, Alberta**

**Participating:**

| | | |
|---|---|---|
| Tony Pickett | (Co-Chair) | RCMP – Ottawa |
| Martin Charette | (Co-Chair) | Sûreté du Québec |
| Ian Kingham | | Ottawa Police Service |
| Paul Batista | | Ottawa Police Service |
| Bernie Murphy | | OPP - Orillia |
| Kelly Anderson | | OPP - Orillia |
| Craig Coughlan | (Chair NTCAC) | Calgary Police Service |
| Jeremy Wittman | | Calgary Police Service |
| Grant Foster | | Saskatoon Police Service |
| Joel Bautista | | Saskatchewan ICE Unit |
| Jim Gainor | | Edmonton Police Service |
| Phil Cutting | | Edmonton Police Service |
| Bill Bosward | | Toronto Police Service |
| John Menard | | Toronto Police Service |
| Jeff Mitchell | | Peel Regional Police |
| Kevin Riel | | Winnipeg Police Service |
| Trevor Ketler | | Winnipeg Police Service |
| Stéphane Denis | | Canadian Police College |
| Ken MacKay | | Edmonton Police Service |
| Kevin Mallay | | RCMP - Halifax |
| Gareth Samson | | Justice of Canada, Criminal Law Policy |
| Marc Moreau | | RCMP – Ottawa |

**Regrets**:

| | |
|---|---|
| John Bilinski | RCMP - Ottawa |
| Carole Matthews | OPP - Orillia |
| John Weigelt | Microsoft Canada |
| Ray  Archer | Canadian Bankers Association – Ontario |
| France Thibodeau | Canadian Police College |
| Bessie Pang | Society for the Policing of Cyberspace |
| Alexander Smith | Attorney General, Crown Law Office – Ontario |
| Dan MacRury | Nova Scotia – Public Prosecution Service |
| Tom Fitzgerald | Toronto Police Service |

| | | |
|---|---|---|
| **Minutes of Meeting** | **NTCAC and CACP**<br>**Meetings**<br>**May 2nd – May 4th, 2012** | |
| | | |
| **Meeting called by:** | S/Sgt. Craig Coughlin (NTCAC) and S/Sgt. Marc Moreau (CACP) | |
| **Type of meeting:** | May 2012 Meeting | |
| **Minutes:** | D/Sgt. Kelly Anderson | |
| | | |
| | **Agenda topics** | **Action by** |
| **Wednesday May 2nd** | **NTCAC Meeting** | |
| | | |
| ***9:00*** | ***Start Welcome by Craig Coughlin and introductions. Review of agenda*** | |
| | (Marc Moreau distributed list of attendees) | |
| | 1. Review of CACP Strategic Plan 2012-2015 | Group Discussion lead by S/Sgt. Marc Moreau |
| | **Discussion on initiatives:**<br>Review of mandate of strategic plan of parent committee.<br>Martin Charette, explained how best to provide support for the strategic plan with a view to the future for the next three years. Incorporating a view from the frontline in the direction of the plan in relation to objectives and goals<br>Issues; Cyber bullying, as a community safety issue for our children<br>Marc Moreau, brought forward a suggestion for a more manageable plan with fewer goals better managing deliverables.<br>Training standards, understudy program brought forward to standardize introduction of | |

| | | |
|---|---|---|
| | new members into e-Crime integration into Canadian Police College training standards<br>Canada one of only countries with a national standard with understudy program and a review of whether it is actually a STANDARD. More formalization of the understudy program across the country. Media releases to generate awareness and better understanding<br>Better articulation of the standards evolving around training for e-Crime investigators/examiners for better understanding across the country and within the CACP. Goal was to prevent improvisation by forensic investigators to create professionalism and improve judicial understanding promoting better case law.<br>**General discussion**.<br>Craig Coughlin. Articulation that understudy was first step shouldn't be considered as final goal but should be viewed as one link in the ongoing professional development of investigators/examiners<br>A roadmap for smaller services who are bringing e-crime services within their services.<br>**CPC is recognized as official training centre for e-crime investigators/examiners based on the strategy**<br>eLearning initiative involving CERT back on track with a demonstration in the fall of what is available. Cost in relation to the training still not finalized, but looking forward to a Canadian focused initiative. Cost effective training to mesh with ongoing professional development of investigators/examiners | |

| | | |
|---|---|---|
| | Also learning through tabletop exercises<br>**TRAINING CPC EA remains important part of strategic plan**<br>*Struggle to maintain adherence to the best practices of search/seizure/analysis*<br>Best Practices for First Responders USSS generally used throughout, resources devoted to developing a Canadian Version.  USSS has been generous in sharing this content.<br>Suggestion standards should encompass all segments involving investigators/examiners involved in search/seizure/analysis<br>RCMP DICE, Advanced First responder program, includes training, equipment allows for resources to be deployed closer to the field, fast tracks the investigation and then ensures triage and maintains proper exhibit integrity, OPP are reviewing program as well in preliminary stages but shows promise.  Definite need for some form of triage.<br>Standards should probably be integrated with Canadian Police College training.<br>**Strategic Goal #2**<br>**i. The Promotion Of Inter-Agency Cooperation In The Prevention, Detection And Investigation Of Technology Based Crime**<br>**ii. The Facilitation Of Public Education** | |

**On Information Security**

**iii The Facilitation Of Public Education On Information Security**

- CACP e-Crime committee linkage with other CACP committees
- Identify other committees and associations with similar mandates including law enforcement and private sector

**Committee Activity:**

- Maintain liaison with appropriate committees and associations including law enforcement and private sector
- Developing partnerships with members of the IT Community
- Development of e-Crime communication strategy
- Inventory of police and public education tools for safe technology usage

**Discussion**

More pro-activity in relation to timely media releases regarding trends in technology & cybercrime Example the ability to trace IP addresses with the IPv6 implementation and IPv4 Network Address Translation (NAT) huge impact on after the fact investigations identifying who is using which IP address. Solutions need to be prepared for to facilitate investigations.

Public education remains priority to maintain our community connections identifying trends/concerns in the arena of public concern.

Next meeting spreadsheet for Subject Matter Experts (SME) within the units of the e-crime community to support community and

| | | |
|---|---|---|
| | investigations.  Facilitating interagency cooperation.<br>**Strategic Goal 3:**<br>**The Establishment Of Proficiency Levels**<br>• Identify training standards<br>• Identify available training including academic, private sector and law enforcement<br>• Identify training tools/web-based training<br>**See previous training notes.**<br>**Strategic Goal  4:**<br>**Linkages with other CACP committees**<br>Discussion regarding Data preservation/Data Retention.  Data Retention not found in the North American structure.  EU directive on Data retention compels member to legislate data retention has met with difficulties.<br>Access to content where legitimate investigative need is present but use of Canadian search authorization not workable/usable.  Suicide risk articulated on a website out of Canada.  No offence for search warrant no jurisdiction for execution outside Canada.  Possibly a PIPEDA letter similar to what is used in child exploitation investigations.  For Canadian ISPs they have annual meetings in which we have been invited to present in this forum to educate on these issues.  Discussion in relation to Bill C30 | |

| | | |
|---|---|---|
| | covering ISPs and not Websites.<br>US stored data/subscriber is bound by legislation regarding disclosure. Typically access is gained through subpoena. Otherwise voluntary disclosure in emergent circumstances permitted at discretion of ISP/Content Hoster. Gareth; USDOJ one of the issues is transporter emergency contact to obtain subpoena on our behalf for ISP/Content host to obtain this emergent information. Additional countries may have similar points of contact that we may be able to utilize<br>Potential for legislative opportunity? but not a quick solution. | |

| | | |
|---|---|---|
| ***1100*** | 2. Search Warrants and Court Procedures | D/Sgt. Kelly Anderson and S/Sgt. Craig Coughlin |
| | In OPP jurisdiction 487 search warrants used, currently trial justices are seemingly concerned with SCOPE of warrant. Officers from tech crime spending days recently on the stand articulating analysis in relation to search warrant authorization.<br>Led to review of suggested wordings in relation to ITO. Remains seizing the tangible of the handset/device from identified civic address. **NOT using** handset/device as location to be searched<br>Areas concentrated on<br>• Communications<br>• Timeline of activity<br>• Ownership<br>• Multimedia, video, pictures sound…<br>• Password access<br>• Device settings software configurations.<br>Assisting officers articulate in the Information to Obtain Search Warrant (ITO) how these points impact their investigation and how these areas allow access for examination within the scope of their search warrant.<br>Meeting with crowns at 720 Bay suggested we appeared to be on right track but there was some suggestion we might be limiting ourselves<br>Additionally no thought had been given to Live forensic analysis under warrant and needed to | **General Discussion** |

| | | |
|---|---|---|
| | be better addressed.<br>Pilot project in conjunction with CIB in which Devices are examined for internet credentials general warrant then obtained to utilize the technique of logging on and capturing data.<br>OPP online content for search warrants at www.e-crime.on.ca/intake<br>Authorizing officials (JPs) inserting their own conditions.<br>Additional issues, push back from the crown in terms of cell phone exams that are overloading them with data that might not be relevant.<br>Crowns are also discussing issues around the scope of search.  Becomes an articulation of why we need to search and access the entire device.<br>Some crown's suggesting second warrant needed to authorize examine the computer.<br>Education of crowns in relation to the evidence how it exists and then careful articulation of the evidence on the stand by the examiner as to why examinations/analysis were conducted | |
| ***1300hrs*** | 3. Searching the Cloud | Group Discussion |
| | DOJ concern is the potential violation of national sovereignty accessing data held in another country.<br>Production order on a company with a presence in Canada, matters not where the | **General Discussion** |

| | | |
|---|---|---|
| | data is held the Canadian country bound to comply.<br>In the context of Live forensics the accessing of data may be easier or more reasonably justified.<br>Bill C30 Lawful Access/Interception<br>Dealing with preservation orders/demands are being set up with the concept of quick freeze/slow access.<br>Preservation demand, no judge reasonable grounds to suspect, data in any ISP in Canada with extensions obtained before judicial authority<br>Compel and ISP on behalf of foreign LE group to preserve data with demand for 90days.<br>Allows Canada to ratify the Council of Europe Convention on Cybercrime.<br>Complicated national sovereignty issues.<br>Details<br>http://www.parl.gc.ca/HousePublications/Publication.aspx?Docid=5380965&File=9<br>Presentation by Craig on some of Bill C30 details/update on status of bill<br>Telecommunications service providers would be entitled to compensation (operational fees) details to be articulated in the regulations.<br>Police officer could request Basic Subscriber Information (BSI), specific circumstances, designated officials, audit trail for documentation. Compensation (operational | |

| | | |
|---|---|---|
| | fees) will apply<br>BSI requests<br>➢ Documentation of requests<br>➢ Regular internal audits<br>➢ 3rd party audits, Privacy Commissioner<br>➢ Freedom of Information (FOI) requests – public interests<br>➢ Penalty for abuse under summary conviction fine not exceeding $250,000.00 | |
| | 4. Computer Emergency Response Team (CERT)<br>• Virtual e-learning opportunities<br>• Live demo of virtual exercise training module | S/Sgt. Marc Moreau<br>Cpl Morgan Bayliss |
| | **DEMO on CERT for tomorrow** | |
| | 5. Lawful Access Update | S/Sgt. Craig Coughlin |
| | | |
| ***1400*** | 6. Canadian Police College – Update | S/Sgt. Stéphane Denis |
| | **Course updates**<br>• Advanced Internet Child Exploitation course focus group recommendations now being implemented<br>• Computer Forensic Examiner course migrated to Windows 7, course long practical scenario, individual submission of report & mock trial<br>• Internet Evidence Analysis Course keeping track with internet usage, trends course sessions being modified as necessary | |

| | | |
|---|---|---|
| | • CMPFOR rescheduled from September 2012 to May 2012 to better meet demand<br>**NEW Courses**<br>• Registry Analysis Workshop<br>• Advanced Computer Forensic Workshop<br>• Both 4 day workshops providing more in depth training on specific topics<br>**OFF Site Course Delivery**<br>• Digital Technologies for Investigators (DTIC), Canadian Internet Child Exploitation (CICE), Registry Analysis Workshop (RAW), Advanced Internet Child Exploitation (AICE) being delivered in Edmonton starting next week<br>• RAW being delivered in Calgary in October 2012<br>• DTIC, CICE, AICE being regularly delivered at Ontario Police College (OPC) starting next week<br>• Discussions with École Nationale de Police du Québec in Nicolet to deliver courses in French<br>**Resources**<br>• Technological Crime Learning Institute (TCLI) regularly requests participation of SME's from field. This participation is essential and appreciated by TCLI in its course delivery<br>• TCLI resources have also been made available to participate in active investigations. | |

| | | |
|---|---|---|
| | Point of Contact for SMEs Carole Matthews and Craig Coughlin to attempt to assist TCLI | |
| | 7. OPP eTracker Demonstration | D/Sgt. Kelly Anderson |
| | • User authentication.<br>• Intake admin, continuity of exhibits<br>• Case management, ability to track case events inserting investigative email into case file via email.<br>• Assignment management<br>• Hierarchical access authorities<br>• DOT net framework coding<br>• Reporting | |
| | 8. Validation of Tools<br>• NIST<br>• US Case Law | **General Discussion** |
| ***1510*** | Tool validation response to RCMP audit report. Is it validation or tool testing<br>National Institute of Standards and Technology (NIST) validation of 80 tools, as well as other organizations, FBI validation of approx. 30-40 tools and the National White Collar Crime Center www.nw3c.org validation of approx. 180 tools are actively engaged in tool validation but perhaps employing different standards/methods.<br>US related information in this area is more advanced both in case law and procedures<br>Push button forensics will lead to problems<br>Reinforce “use a tool; understand its function; and validate it’s results by other means. | |

| | | |
|---|---|---|
| | Lengthy discussion boiled down to the necessity of validating results and due diligence on tool source | |
| *16:00* | Meeting adjourned | |
| **Thursday May 3rd** | **NTCAC/CACP Combined Meetings** | |
| | | |
| ***9:00*** | ***Start*** | |
| | Presentations: | |
| | 1. Department of Justice<br>• Update on G8 High Tec Crime Sub Group (HTCSG) meeting – March 2012<br>• Update on meetings in Washington DC with DOJ and FBI | Mr. Gareth Sansom |
| | 2. Sûreté du Québec<br>• Update on ARIN (American Registry for Internet Numbers) and AGWG (ARIN/Government Working Group)<br>• Recent meeting in Vancouver – April 2012 | Lieutenant Martin Charette |
| | 3. RCMP Integrated Technological Crime Unit - Edmonton<br>• Cell phones<br>• Challenges | Sgt. Jeff Cameron |
| | 4. IBM Forensic Triage Tool | IBM Representative<br>Scott Michael Padgett |

| | | |
|---|---|---|
| | 5. Live Demo from the Computer Emergency Response Team (CERT), Carnegie Mellon University, Pittsburgh, PA on the following learning opportunities:<br>a. E-learning opportunities. The CERT has agreed to make available a large number of on-line training to our digital crime investigators. The prices for these courses have not yet been set but will be considered highly affordable based on similar courses offered at commercial institutions.<br>b. The "Xnet" virtual training exercise module is an excellent example of the innovative learning tools the CACP E-Crime Committee is looking to make available to the Canadian law enforcement community. It offers quality training for cyber investigators with no travel costs associated to this type of learning opportunity.<br>These learning opportunities offer real cost-efficient alternatives in regards to the specialized training required by our investigators. | |
| | 6. Local Crown Issues | Mr. Phil Cutting |
| **Friday May 4th** | **CACP Meeting** | |
| ***9:00*** | ***Start*** | |
| | 1. Review 2010 Annual Report (submitted at the CACP conference in Windsor Aug 2011) | Supt Tony Pickett<br>S/Sgt Marc Moreau |
| | 2. Law Enforcement Due Diligence Recommendations to ICANN (Update in efforts of LE to gain a voice in the Internet governance). | S/Sgt Marc Moreau |

| | | |
|---|---|---|
| | a. Attendees provided with a copy of his recent post-travel report to the ICANN meeting in Costa Rica, 2012 11/15<br>b. There is agreement in principle on 10 of the 12 LE Recommendations. The outstanding 2 require more work. | |

| | | |
|---|---|---|
| | 3. Strategic Plan 2012-2015<br>Following the discussions with the NTCAC and the CACP E-Crime, S/Sgt Moreau will prepare a draft of a new Strategic Plan. | S/Sgt Marc Moreau |
| | 4. ARIN – Results of the recent Policy Proposal at the ARMIN meeting – Vancouver April 2012 (policy 2011-07 Compliance Requirements<br>https://www.arin.net/policy/proposals/2011_07.html | Lieutenant Martin Charette |
| | 5. Discussion was held in regards to the following 3 questions we have been asked to answer by the Cyber Crime Working Group (CCWG) of the Federal/Provincial/Territorial (F/P/T):<br>1) Is encryption a significant problem for law enforcement?<br>2) Are there "work arounds" or solutions that currently address this problem?<br>3) Are there concerns that you have regarding these solutions that could be addressed by changes in the law?<br>Following a group discussion it was agreed that S/Sgt Marc Moreau and Gareth Sansom (DOJ) would work together to provide an appropriate answer to the CCWG | Supt Tony Pickett<br>S/Sgt Marc Moreau |
| | 6. Discussed the RCMP Audit of the Technological Crime Program<br>• Requirement for strategic vision of program (and others across Canada)<br>• Can demonstrate that there are provisions for First Responder, | Supt Tony Picket |

| | | |
|---|---|---|
| | Advanced First Responder (DICE) and more advanced Subject Matter Experts (SME)<br>• Can demonstrate the domestic collaboration (NTCAC/CACP E-Crime)<br>• Can demonstrate the international collaboration G8, SAG, ICANN, ARIN | |

| ***ACTION ITEMS*** | **Comments** | **Assigned To** |
|---|---|---|
| 1.Identify priorities for 2013 | Members are encouraged to think about strategic priorities for the CACP E-Crime/NTCAC for next year. | TBD |
| 2.Strategic Plan 2012-2015 | A draft document will be prepared based on the discussions from these meetings. | S/Sgt Marc Moreau |
| 3. Proposed Resolutions | The following Resolution for 2012 (in preparation for the CACP Annual conference, Sydney NS Aug 19-22, 2012) had been distributed to the NTCAC/CACP E-Crime members for comments:<br>We are asking the CACP to: Support the requirement for a National Cybercrime Strategy to disrupt and neutralize Canadian-based cybercrime, through means centered around:<br>• The development of interagency capacity for increased coordination and collaboration;<br>• The identification of interprovincial and international operational plans to increase the effectiveness of law enforcement initiatives;<br>A national harmonized data collection point for Cybercrime complaints / incidents. This could include the existing Canadian Anti-fraud Centre (CAFC) as a strategic partner in this endeavour | S/Sgt Marc Moreau |
| | | |
| **Round Table** | | |
| | | |
| | | |
| | | |

Dated: 2012-06-05 – Reviewed by S/Sgt Marc Moreau

# Appendix "D" - Success Stories 2012

1-) The Saskatchewan Internet Child Exploitation Unit (SASK ICE) was involved in an investigation involving a male suspect. This investigation was part of a joint investigation that involved the Edmonton Police Service (EPS). It was determined the accused was interested in a sexual encounter with a minor.

The investigation determined the suspect was living with his girlfriend and her two year old daughter. This discovery resulted in the joint Saskatchewan ICE and Edmonton PS to precipitate the arrest of the suspect. He denied ever touching or doing anything inappropriate with his girlfriends young daughter but did admit to fantasizing about the child. Ever since he received the picture asking him to have sex with the girls, he was totally transfixed with the undercover agent and the possible meeting with young girls. Investigators believe if the suspect was not removed from this relationship, there would have been a high probability of sexual abuse.

The suspect was charged with 3 counts of Conspiracy to Commit Sexual Assault, 3 counts of Conspiracy to Commit Sexual Interference, production of Child Exploitation material and Possession of Child Exploitation material.

---

2-) From the Toronto Police Service (TPS):
Case History: The accused (male) and victim (female) were having marital problems. Investigators found the victim in her bathtub where she had apparently drowned. Several elements surrounding the case arose the suspicion of the investigators. As a result, the Homicide Unit seized the electronic devices from the accused. The autopsy on the victim revealed that she had been drugged. Investigators hoped that the examination of the computer equipment could provide some evidence of foul play that could be a contributing factor in this death.

The initial examination of several exhibits did not yield any results of value. The examination rested on the forensic retrieval of evidence from the computer. An intensive manual analysis of the raw data on the computer would be required. Through a carefully constructed keyword search and an analysis of several temporary files, evidence of Internet queries was found centered on administering drugs to potential victims.

Forensic examiners conducted research into the file structure of the operating system. Forensic examiners performed further calculations and developed a tool to run against the image of the seized computer. This allowed the fragments of the deleted files to be displayed. As a result, Facebook log-ins, times and dates were successfully extracted. As a direct result of the information that was provided by the Forensic investigators the accused was arrested and charged with First Degree Murder.

3-) From the Toronto Police Service (TPS):
Case History: The accused (male) was having sexual relationship with a pre-teen victim (female). During the relationship, the male sent many vulgar and sexual emails to the victim. After some time, the sexual assault came to light and investigators seized the computer equipment of the accused.

Prior to Police arrival, the accused wiped the contents of all of his digital devices rendering little chance of obtaining any evidence. Any hope centered on the victim's digital device but unfortunately the victim, unknowingly, erased all messages and emails sent from the accused. Furthermore, the victim modified her digital device in such a way that made any use of automated tools impossible and had overwritten her email storage in an attempt to forget what she had endured.

The Tech Crime investigators worked diligently and were successful in recovering deleted communications. The sexual and vulgar emails which the accused had sent were recovered along with the dates and times of their arrival. The database contained the header information from the emails including IP addresses. Officers further located the victim's personal diary which gave further insight into the sexual assaults. The evidence obtained was crucial to the investigation and the accused is currently standing trial for his crimes.

4-) From the Toronto Police (TPS):
Officers in 51 Division were investigating a charge of voyeurism where the accused was using his smartphone to capture video of unsuspecting female victims. An arrest was made and the smartphone was seized and submitted for analysis.

The forensic retrieval of evidence from the digital device can be a challenge. There are limited formalized methodologies or dedicated software for this purpose. Forensic examiners from the Intelligence Division, Technological Crime Section were able to author a new forensic method to extract data from the smartphone. Other devices had failed to extract a physical image so examiners used file system data and a memory card to retrieve deleted video files showing the offence. 51 Division were looking to prove this phone was connected to a computer in the residence of the accused, both to show ownership as well as to further their investigation to that residence. Forensic examiners were able to extract key parts of the digital device’s file system where they located GPS data. This GPS data proved that the phone had had connected to a Wi-Fi signal at a GPS coordinate directly linked to the residence of the accused. Officers were able to show the exact Wi-Fi SSID name the phone was connected to and, with this data, Officers from 51 Division were able to confirm the same Wi-Fi SSID in the residence of the accused. Based on the evidence extracted the accused was charged and is currently facing trial.

5-) The Calgary Police Service (CPS), Integrated Child Exploitation (ICE) team conducted an investigation which led to a suspect who is an international cyber security expert. They seized several computers and through the computer forensic analysis completed on the seized computers, it was discovered that the computers contained child exploitation material and evidence of luring. The suspect was charged accordingly. The suspect hired a high profile lawyer and he obtained the services of 2 computer science professors from the University of Calgary. They testified that a computer virus was responsible for downloading of the child exploitation material. The ICE team lacked the expertise to combat this line of reasoning and utilized the services of a member of the CPS Tech Crime Team. The member who has taken courses in malware analysis looked at the viruses that were present. He conducted extensive testing on each virus in virtual and live environments to see exactly how the virus behaved. He then decompiled the viruses and looked through the code line by line. He was sworn in as a malware expert. He provided detailed and professional testimony. The Judge sided with the Constable saying that his evidence was much more thorough than that of the 2 professors and convicted the suspect. He was sentenced to 3 years in jail.

6-) In early 2012 an innocent bystander was stomped to death by a group of white supremacists in Calgary. During the course of the homicide investigation several requests were made to the CPS Tech Crime Team (TCT) for assistance. One request was to conduct several strategic acquisitions. Due to the extensive nature of their request the TCT had to update several of their Standard Operational Procedures (SOPs). Publicly available tools were used in this investigation. As well, specialized tools were also developed. Forensic analysis was completed on several digital devices. The data collected was extremely useful in eventually charging several people in this complex case. Some of the tools developed in this investigation have also been used in other homicide files.

7-) The Calgary Police Service (CPS) conducted a homicide early in 2012 in which the investigator seized a digital device. The digital device and some other components were damaged and rendered it inoperable. Members of the CPS Tech Crime Team (TCT) had earlier completed training in this highly specialized area. The TCT members successfully replaced the damaged components of the digital device seized and this allowed the proper access to the device. The TCT members were then able to extract the valuable evidence pertinent to the homicide investigation.

8-) From the Edmonton Police Service (EPS):
In September 2011 the Edmonton Police Service Technological Crimes Unit (EPS TCU) received a request for assistance in a serious sexual assault investigation where the complainant had been violently sexually assaulted with a weapon, and then subsequently suffered an aggravated assault after reporting the original incident to police. Detectives believed key evidence was contained on a digital device that was locked by a passcode and inaccessible to investigators. At the time of the request, no established forensic techniques or tools existed to defeat the protections on this particular device. Members of the EPS TCU began research and development efforts in an attempt to find a solution, testing and modifying specialized computer programs developed in a country abroad. TCU efforts ultimately culminated in the application of a risky but necessary procedure against the device. This procedure successfully extracted the passcode from the device while preserving the integrity of the data contained therein. Using the extracted passcode members of the TCU were then able to extract the key evidence from the unlocked device, as well as additional evidence relating to the attempted murder investigation.

Members of the EPS TCU had consulted with experts from across North America with respect to this file, and the consensus was that this type of technique had never been successfully performed in a criminal investigation. TCU efforts led not only to a successful outcome within the scope of this investigation, but also to the development of an innovative new technique that will benefit our partners in law enforcement worldwide. Details of the procedure have already been shared with forensic examiners from other Canadian law enforcement agencies to assist in their own investigations.
This matter remains before the courts.

9-) From the Edmonton Police Service (EPS):
In February 2012, the Edmonton Police Service (EPS) conducted a high profile investigation into a homicide that resulted in a successful prosecution.

In October 2008 the victim was lured via an online dating web site to an Edmonton garage where he was bludgeoned to death and dismembered by the accused. What began as a missing persons investigation took a horrific turn when members of the EPS Technological Crimes Unit (TCU) identified what appeared to be remnants of a deleted document on the computer of the accused. Nearly 50 pages of text were extracted and pieced together by TCU members, recreating the document that would become strong evidence in a highly sensationalized case. TCU members spent months working on the investigation, which involved multiple search warrants and forensic examinations of several computers. MLAT requests were also completed in December of 2008 and forwarded through Ottawa in January 2009 for several social media company giants. The requested records were finally received by the EPS 17 months later, June 2010, at which time a second stage of follow-up analysis had to be performed by TCU members. In November of 2010 Defence Counsel attempted to have the forensic examination of the laptop excluded as an unreasonable search under S. 24(2) of the Charter. The Court held that once a warrant authorizes a search that includes a computer, absent some form of limitation in the warrant, the entirety of the computer's contents could be examined, establishing valuable case law for the Crown and law enforcement in Canada. During the jury trial in Alberta's Superior Court in April of 2011, Tech Crime members testified for two days before two packed courtrooms (one courtroom was set aside just to house the hundreds of news reporters, connected to the main courtroom via an audio feed).

The accused is currently serving a life sentence with no chance of parole for 25 years.

10-) From the Sûreté du Québec

The Sûreté du Québec began an investigation in a case of a person in possession of child exploitation material.
A neighbour of the suspect reported to have found such files on a DVD. Investigators obtained a search warrant and upon executing the search of the suspect's residence they seized computers and other digital media devices. The devices were analyzed by the the Sûreté du Quêbec's Technological Crime Unit and several child exploitation graphics and video files were found. During the analysis of the seized devices, the Sûreté du Québec also discovered graphics and videos implicating a yet to be identified victim of a sexual assault. As a result, a second search warrant was obtained for the production of child exploitation material.
The examiner discovered that the suspect was using a chat program to talk about the aggressions. The extracted log files from that program revealed that the suspect had been distributing child exploitation files along with the victim's graphics and video files.
Meanwhile, the Sûreté du Québec Victim Identification within the Technological Crime Unit has been working with Interpol to verify international databases to determine the possibility of distribution of child exploitation material. The results have shown that some of the files had been located in Australia and Romania. A third search warrant was obtained for the distribution of child pornography. Once again, the examiner analysed the seized items for the distribution of child exploitation. The examiner determined that the suspect was using peer-to-peer software that was sharing child exploitation material with other Internet users including the victim's graphics and video files.
The thorough analysis allowed the Sûreté du Québec to identify the victim and share this information with the appropriate law enforcement organizations. Thankfully, the victim in this case was rescued and the suspect was charged with possession, distribution, production of child exploitation material and sexual assault.

This case is still pending.

11-) The RCMP Technical Analysis Team (TAT), Ottawa, continues to offer leading edge expertise with regards to the advanced analysis of digital devices. Assistance is provided to all levels of local, municipal, provincial, and federal law enforcement partners in Canada, along with assistance to international law enforcement agencies. In addition to performing the complex forensic analysis of numerous digital devices each year, advanced research and development into flash memory data recovery and damaged device repair is conducted to address unique cases that are submitted.

Assistance was provided during the investigation of the well-publicized “Shafia” family murders in Kingston, Ontario. Members of TAT were able to perform advanced analysis of the navigation system, extracting and interpreting saved waypoints near the scene of the crime in Kingston. Expert witness testimony was provided during the trial in November 2011, which ultimately lead to the guilty verdict on four counts of first-degree murder for each of the three defendants in January 2012.

Although still before the courts, expert testimony was recently given during the preliminary hearing for an impaired driver and driving while texting case that resulted in the deaths of two young women. Charges of criminal negligence causing death (2 counts) are being prosecuted against the driver who was a young offender at the time. Significant text messaging evidence within the locked device was read out in court that detailed the sequence of events leading up to the collision, followed by the horrific aftermath.
Assistance to a municipal transit authority was provided following the arrests of suspects involved in an estimated $250,000 transit pass fraud. A locked digital device was analyzed that contained foreign language emails and high-resolution photographs of transit passes used for counterfeiting. The scheme involved the photographing of new transit pass details, with counterfeit passes coming from a foreign country. Canadian suspects are still before the courts, while foreign nationals on student visas have been deported.

In another case that is still before the courts, a municipal sex crimes unit sought the assistance of TAT in extracting the data from a locked digital device to support charges of child luring and possession of child exploitation material. This case was the first of its kind seen by TAT, with numerous call logs, text messages, and hundreds of images being recovered. The vast amount of evidence found within the device identified other potential victims allowing additional charges to be laid.

In yet another case, TAT was able to utilize specialized equipment to extract the data from a USB thumb drive that was considerably damaged. Through special tools and techniques, TAT was able to successfully extract all of the data that was then reconstructed into an intact file system. Hundreds of child exploitation images from the Internet were recovered, along with key evidence supporting criminal charges relating to the production of child exploitation material.

The RCMP Forensic Utility & Research Team (FURT), Ottawa provided assistance to the RCMP International Operations Branch, Ottawa with regards to a major investigation of alleged illegal human trafficking/smuggling in the recovery of passwords and encrypted data.

Over the past year, the RCMP Technological Crime Program conducted the forensic analysis of numerous digital devices in relation to a high profile National Security investigation. The complexities of the matter required the secondment of personnel from across the country. The analysis corroborated information gleaned through intercepts during the investigation and uncovered new evidence for the investigators. The matter remains before the courts.

12-) From the RCMP Winnipeg:

Back in early 2010, a search warrant was executed at a residence in the community of Iqaluit, Nunavut in regards to a Controlled Drugs and Substances Act investigation. While examining exhibits that were seized during this search, one of the attending investigators from the Winnipeg Tech Crime Unit, discovered a number of images on a USB drive that constituted child exploitation material. This illegal material appeared to involve local victims and was surreptitious in nature. The search warrant was executed at a residence in the community of Iqaluit, Nunavut. The “D” Division Integrated Child Exploitation Unit (ICE) and Nunavut Serious Crime Unit (SCU) subsequently became involved.

After a search warrant was obtained to search for child exploitation evidence, the RCMP Tech Crime investigator conducted a forensic examination of the accused's items, which consisted of laptops and USB drives. He recovered copies of the images in various locations as well as link files demonstrating that the images were viewed on one of the laptops belonging to the accused.

Through the course of this investigation, the victims were identified and subsequently interviewed by the lead investigator from Nunavut SCU. Although the victims did not have any knowledge of the images, numerous disclosures were made. The accused had sexually abused and exploited his daughters and some of their friends over the course of a number of years.

The accused was subsequently arrested and charged with numerous counts of sexual offenses, as well as possession of child pornography. The forensic evidence and information was subsequently organized in a manner that was suitable for defense counsel, as full disclosure of the images was requested.

In the spring of 2012 the accused plead guilty to 4 counts of sexual assault and 2 counts of sexual interference (in addition to drug offenses). The accused was sentenced to 5 years for these offenses.

13-) A 16 year old girl reported to the Ontario Provincial Police (OPP) that she was sexually assaulted at knifepoint in an Ontario provincial park. A total of 357 persons were canvassed and 23 persons of interest were identified and interviewed. The same girl reported another sexual assault (by the same suspect but different time / place) to the Waterloo Regional PS. The girl identified the suspect during the second report but did not advise the OPP that the suspect was the same person as the first reported assault.

Waterloo Regional PS contacted the OPP to communicate information about the identity of the possible suspect in relation to the first alleged assault. As a result, the OPP executed a search warrant at the suspect's residence and seized 2 computers, 2 thumb drives and 2 CDs. The complainant also reported sending pictures of herself to the suspect and that he would be in possession of child exploitation material.

During the examination of the suspect's computers, several chats between the alleged victim and suspect were found. The chats were very graphic in nature and described what the girl had sexually done to the “suspect” and what she wanted to do to him (sexually) in the future. She provided her home address to the suspect and invited him over (where the second alleged assault took place). The last chat was dated the day that the alleged victim and her mother attended the Waterloo Regional PS to report the alleged sexual assault. As a result of the chats, the "victim" was re-interviewed and ultimately charged with public mischief. The suspect was not charged for the assault(s) and no child pornography was found on his computers. This is an example of how an un-biased electronic crime investigation can also assist with exonerating individuals.

14-) The Ontario Provincial Police (OPP) Technological Crime Unit assisted with a sexual assault involving a 14 year old female and male in his 30’s. The initial examination of the victim's phone corroborated her complaint in relation to “sexting” and photographs. As a result, the male was arrested and three electronic devices were seized from him; one of the devices was a damaged phone. Advanced forensic techniques were utilized to conduct an examination of the damaged phone which successfully yielded a photograph of an additional victim. This information was passed onto the investigating officer, which lead to the identification of the victim who was subsequently interviewed. The victim was also sexually assaulted by the male accused. The photograph of the second victim was stored in an unlikely place that could have been easily missed if proper forensic techniques were not utilized. The location of the photograph also shows some degree of sophistication by the accused in relation to his ability to “hide” the photograph. Investigations like this one highlight the extraordinary work the members of specialized Tech Crime Units can conduct to assist with criminal investigations and ultimately the identification of victims.

15-) The Ontario Provincial Police (OPP) Technological Crime Unit (TCU) and the Child Sexual Exploitation Unit routinely work together to investigate matters relating to child sexual exploitation and abuse. It is extremely important that investigators in these units have a high degree of technical knowledge. In one such instance, an accused was charged with making available, possession and accessing child pornography. The issue at trial had to do with the whether or not the accused had the *mens rea* to commit the offence through his use of peer to peer sharing using a specific application. A large part of the job of Technical Investigators is the ability to articulate evidence during court proceedings. In this scenario, a member of the TCU was successfully able to explain to the court, through expert testimony, how the program works and how the accused altered advanced settings on his computer to change sharing properties. The accused was shown to have manually altered default program settings to optimize file transfers without preventing or blocking the sharing of files from the computer system. Due to the excellent understanding of the technical aspects of the investigation by the investigators and the ability to articulate evidentiary findings in relation to the accused’s computer system, the accused was found guilty on all counts.