



## ARCHIVED - Archiving Content

### Archived Content

Information identified as archived is provided for reference, research or recordkeeping purposes. It is not subject to the Government of Canada Web Standards and has not been altered or updated since it was archived. Please contact us to request a format other than those available.

## ARCHIVÉE - Contenu archivé

### Contenu archivé

L'information dont il est indiqué qu'elle est archivée est fournie à des fins de référence, de recherche ou de tenue de documents. Elle n'est pas assujettie aux normes Web du gouvernement du Canada et elle n'a pas été modifiée ou mise à jour depuis son archivage. Pour obtenir cette information dans un autre format, veuillez communiquer avec nous.

This document is archival in nature and is intended for those who wish to consult archival documents made available from the collection of Public Safety Canada.

Some of these documents are available in only one official language. Translation, to be provided by Public Safety Canada, is available upon request.

Le présent document a une valeur archivistique et fait partie des documents d'archives rendus disponibles par Sécurité publique Canada à ceux qui souhaitent consulter ces documents issus de sa collection.

Certains de ces documents ne sont disponibles que dans une langue officielle. Sécurité publique Canada fournira une traduction sur demande.

<p><b>Canadian Association of Chiefs of Police</b> Leading Progressive Change in Policing</p>		<p><b>L'Association canadienne des chefs de police</b> À l'avant-garde du progrès policier</p>
---	---	--

## Electronic Crime Committee 2010 Annual Report



## **TABLE OF CONTENTS**

Table of Contents .....	2
2010 Message from the Chair .....	3
Committee Mandate/Objective .....	5
Dates/Overview of Meetings .....	6
Summary of Initiatives/Activities 2009/2010: .....	10
<b>Resolution 2010-01</b> .....	11
<b>Activities Planned/Significant Dates 2010/2011 :</b> .....	15
<b>COMMITTEE MEMBERS LIST:</b> .....	16
Tom Pownall .....	16
Ken MacKay .....	17
Dan Killam .....	18
Thomas Fitzgerald .....	20
Al Tario .....	21
Grant Foster .....	22
Martin Charette .....	23
Ray Archer .....	24
<b>ASSOCIATE MEMBERS</b> .....	<b>25</b>
John Weigelt .....	25
Bessie Pang .....	26
<b>TECHNICAL ADVISORS</b> .....	<b>27</b>
France Thibodeau .....	27
Dan MacRury .....	28
Gareth Sansom .....	29
Alex Smith .....	30
Marc Moreau .....	31
<b>Appendix "A"</b> .....	32
CACP E-crime Meeting January 7, 2010 Toronto, Ontario .....	32
<b>Appendix "B"</b> .....	39
CACP E-crime Meeting May 6/7, 2010 Halifax, Nova Scotia .....	39

---

## **2010 MESSAGE FROM THE CHAIR**

I am pleased to report on the 2009/2010 activities of the CACP E-Crime Committee. We continue to follow our Strategic Plan as a road map to ensure that our Committee activities remain aligned with our committee mission and the goals and objectives of the CACP. We also continue to liaise with other CACP Committees.

The committee continues its efforts to broaden its membership and achieve enrolment that is truly national in scope and composed of Canadian police leaders, private sector members, prosecutorial experts and technical advisors. The Committee currently includes police representatives from the RCMP, OPP, Sûreté du Québec, as well as Toronto, Ottawa, Saskatoon and Edmonton Police Services. Related Justice Representatives include Justice Canada, Public Prosecution Service of Nova Scotia, Crown Law Office of Ontario and Canadian Police College. Private sector, representatives include the Canadian Bankers Association, Society for the Policing of Cyberspace and Microsoft Canada. The Electronic Crime Committee held three meetings this year. A winter meeting was held in January in Toronto, a spring meeting was held in May in Halifax and the third meeting was held immediately prior to the CACP Annual Conference in Edmonton in August.

This year the Committee sought opportunities to provide strategic leadership in matters related to Internet governance. The committee received and reviewed a document prepared by the broader international policing community, including the Australian Federal Police, the New Zealand Police, the Serious Organized Crime Agency in the UK, the Federal Bureau of Investigation in the US and the Royal Canadian Mounted Police. This document identifies a number of due diligence recommendations in relation to providing a safe and secure environment for the Internet. The above described law enforcement agencies have submitted these recommendations to the Internet Corporation for Assigned Names and Numbers (ICANN). Since the initial submission to the ICANN, the recommendations have been endorsed by the G8 Roam Lyon Group High Tech Crime Sub-Group, the Strategic Alliance Cyber Crime Work Group, Interpol and the Council of Europe. The CACP Electronic Crime Committee has reviewed the recommendations and this year's annual report contains a resolution seeking the support of the CACP executive and formal endorsement of the CACP by way of a letter to the Internet Corporation for Assigned Names and Numbers.

The development of national standards in relation to electronic crimes is an on-going activity of the committee. This year the committee has worked with the CACP National Tech Crime Advisory Sub-Committee and advanced work in relation to national standards relating to digital forensic methodology, disclosure and report writing. We expect that this work will continue through 2010/2011.

**Many of the Committee's member organizations have advanced cyber crime capabilities. However, it is consistently reported across the member organizations that they face service shortfalls, backlogs and capacity issues. Many of the specialized technical enforcement programs are under-resourced and carrying increasing workloads which could compromise e-crime investigations.**

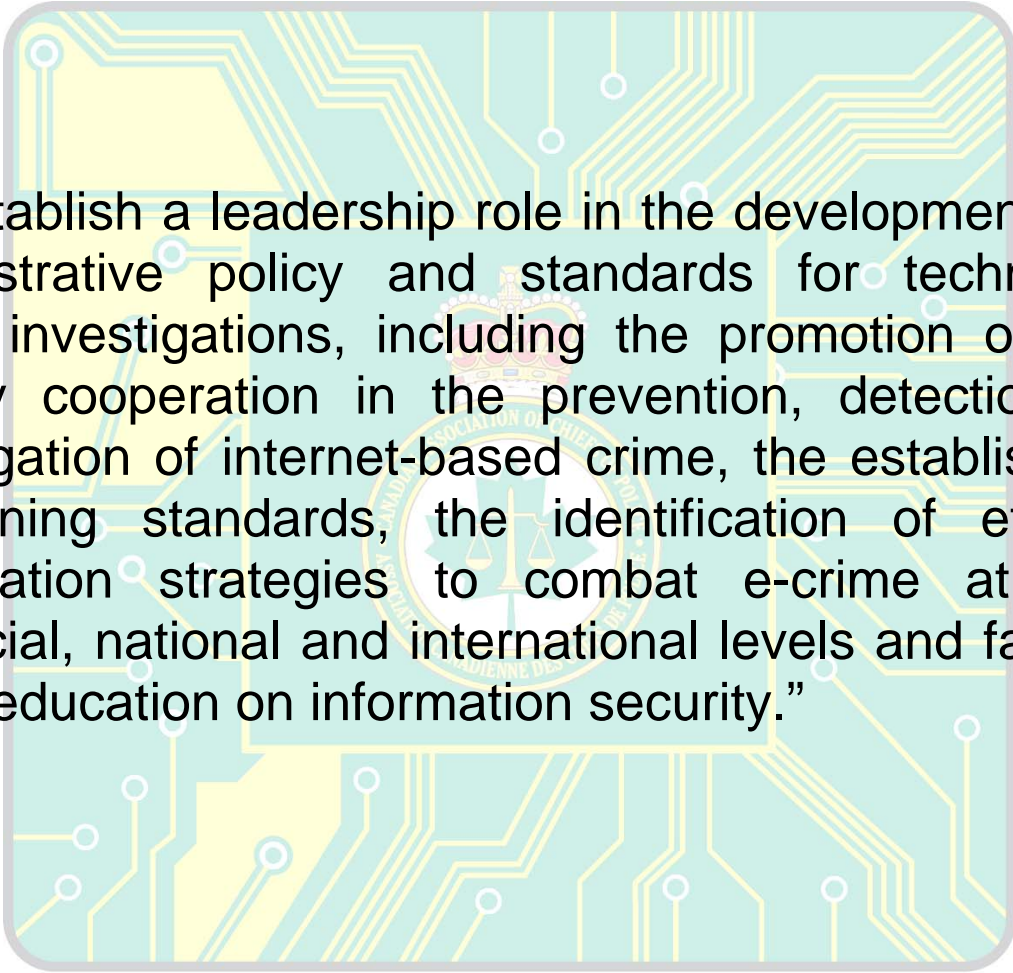
There are a number of emerging challenges in relation to electronic crimes and Canada's police services must work together to develop a coordinated, effective response. In 2010 the E-Crime Committee continued to be an excellent venue to share knowledge, skills and abilities to enhance strategies in combating E-Crime. In 2010, 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 that there is a requirement to ensure that new funding initiatives by all levels of government include sufficient allocations for specialized technical investigative services. 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.

In 2010, Chief Superintendent Kate Lines, Co-Chair of the committee, announced that she would be retiring from service with the OPP and relinquishing her role as Co-Chair of the E-Crime Committee. The committee would like to wish Kate all the best in her retirement and thank her for her years of professionalism and dedicated service as a member and Co-Chair of the E-Crime Committee.

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 and support.

Superintendent Tom Pownall  
Royal Canadian Mounted Police

## COMMITTEE MANDATE/OBJECTIVE



“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.”



CACP e-Crime Committee

## **DATES/OVERVIEW OF MEETINGS**



The e-Crime Committee meets approximately every 4 months in each calendar year in different parts of Canada. Committee members are currently hosting the meetings and any expenses incurred are borne by the host. CACP Board of Directors provides funds to offset these expenses of non-police members to attend.

The winter 2010 meeting of the e-Crime Committee was held on January 7, 2010 in Toronto, Ontario. In attendance were:

### **Winter 2010**

#### **Participating:**

Tom Pownall (Co-Chair)	RCMP - Ottawa
Kate Lines (Co-Chair)	OPP - Orillia
Martin Charette	Sûreté du Québec
Grant Foster	Saskatoon Police Service
Ken MacKay	Edmonton Police Service
Tom Fitzgerald	Toronto Police Service
Ray Archer	Canadian Bankers Association – Ontario
John Weigelt	Microsoft
Dan Rajsic	OPP – Orillia
Shawn Nash	OPP – Orillia
Marc Moreau	RCMP - Ottawa

#### **Participating via teleconference:**

Bessie Pang	Society for the Policing of Cyberspace
France Thibodeau	Canadian Police College
Alexander Smith	Attorney General, Crown Law Office – (Ont)

#### **Regrets:**

Al Tario, Ottawa,	Ottawa Police Service
Peter Hourihan	RCMP - Winnipeg
Gareth Samson	Justice of Canada, Criminal Law Policy
Dan MacRury	Nova Scotia – Public Prosecution Service

Items discussed included:

- Observed a moment of silence in honour of Cst. Eric Czapnik, Ottawa Police Service who lost his life while performing his duties
- Overview of the Internet Corporation for Assigned Names and Numbers (ICANN) organization
- Bill C-46 Update
- Bill C-47 Update
- Mobile Device Advancements
- Economic Impact of Cyber Security
- Major Events Preparedness (2010 Winter Olympics, G8-G20)

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



## Spring 2010

The spring 2010 meeting of the e-Crime Committee was held on May 6/7, 2010 in Halifax, Nova Scotia . In attendance were:

### **Participating:**

Tom Pownall (Co-Chair)	RCMP – Ottawa
Grant Foster	Saskatoon Police Service
Dan Killam	RCMP - Edmonton
Martin Charette	Sûreté du Québec
Gareth Samson	Justice of Canada , Criminal Law Policy
Marc Moreau	RCMP – Ottawa
Shawn Nash	OPP - Orillia

### **Participating via teleconference:**

Bessie Pang	Society for the Policing of Cyberspace
-------------	--

### **Regrets:**

Kate Lines (Co-Chair)	OPP - Orillia
Ken MacKay	Edmonton Police Service
Al Tario, Ottawa,	Ottawa Police Service
Tom Fitzgerald	Toronto Police Service
Ray Archer	Canadian Bankers Association – Ontario
France Thibodeau	Canadian Police College
Michael Eisen	Microsoft
Randy Robar	RCMP – Charlottetown
Alexander Smith	Attorney General, Crown Law Office – (Ont)
Dan MacRury	Nova Scotia – Public Prosecution Service

Items discussed included:

- Presentation by RCMP members of the Halifax, Atlantic Regional Technological Crime Integrated Unit (ARITCU) on the digital forensic methodology, disclosure and report writing
- Partnership initiative update – Simon Fraser University and POLCYB (Society for the Policing of Cyberspace)
- Internet governance initiative – Due diligence recommendations presented to ICANN (Internet Corporation for Assigned Names & Numbers) on behalf of the international law enforcement community
- National Tech Crime Advisory Committee - Legislative initiatives and concerns

- CERT (Computer Emergency Response Team) Virtual training. Valuable on-line training opportunity made available by the FBI
- Validation of specialized technical tools
- FastScan software – Issues and concerns
- Virtual worlds and crime. Presentation by Mr. Gareth Sansom, Dept of Justice.
- Criminal use of the Domain Name System (DNS)
- Resolution/Next steps

Full Meeting minutes are available in **Appendix “B”** of this report.

## **SUMMARY OF INITIATIVES/ACTIVITIES 2009/2010:**

- Concluded work to review and support law enforcement due diligence recommendations regarding Internet governance.
- Circulated three Strategic Alliance Cyber Crime Working Group information bulletins.
- Initiated work on a national standard forensic methodology.
- Assessed emerging risks and potential for criminal exploitation of virtual worlds.
- The Committee continues to work with the operational members of the National Tech Crime Advisory Committee (NTCAC).

## Resolution 2010-01

### *Due Diligence & Other Recommendations to ICANN (Internet Corporation for Assigned Names and Numbers)*

#### **Commentary**

The Internet Corporation for Assigned Names and Numbers' (ICANN) was formed in 1998. ICANN is an international not for profit public-benefit corporation dedicated to keeping the Internet secure, stable and interoperable. ICANN promotes competition and develops policy on the Internet's unique identifiers.

The international law enforcement community has consulted with Internet registrars and drafted and proposed a series of due diligence recommendations to ICANN in the interest of promoting ICANN's mission to keep the Internet secure, stable and interoperable.

Representatives of Canadian law enforcement and their partners on the CACP Electronic Crime Committee have reviewed the due diligence recommendations and have determined that their application and implementation would reduce opportunities for on-line crime and enhance on-line security.

#### **Media Lines**

- Law enforcement agencies from the US, UK, Canada, Australia and New Zealand have proposed a series of recommendations for amendments to the Internet Corporation for Assigned Names and Numbers' (ICANN) Registrar Accreditation Agreement (RAA).
- The principle aim of these proposals is to implement stronger controls around domain name registration and ensure a rigorous regulatory framework to govern ICANN's contracts with domain registrars. They include requirements for effective due diligence on accredited registrars, controls to ensure more accurate WHOIS information and availability for Law Enforcement.
- The international law enforcement community views these recommendations as vital in preventing crimes involving the Domain Name System and the recommendations are considered to be necessary to aid in the prevention and disruption of efforts to exploit domain registration procedures for criminal purposes.
- The CACP supports these recommendations in furtherance of a safe and secure Internet and to promote effective crime prevention and criminal investigations

## RESOLUTION

2010-01

### ***Due Diligence & Other Recommendations to ICANN***

*Submitted by the e-Crime Committee*

**WHEREAS** Criminals may seek anonymity and exploit the Domain Name System in furtherance of illicit acts

**WHEREAS** In October 2009, a series of recommendations for amendments to the Internet Corporation for Assigned Names and Numbers' (ICANN) Registrar Accreditation Agreement (RAA) was proposed to ICANN by law enforcement agencies from the US, UK, Canada, Australia and New Zealand;

**WHEREAS** The recommendations are considered to be necessary to aid in the prevention and disruption of efforts to exploit domain registration procedures for criminal purposes.

**WHEREAS** The international law enforcement community views these recommendations as vital in preventing crimes involving the Domain Name System;

**WHEREAS** The principle aim of these proposals is to implement stronger controls around domain name registration and to ensure a mandatory and rigorous regulatory framework to govern ICANN's contracts with domain registrars.

**WHEREAS** The recommendations include requirements for effective due diligence on accredited registrars, controls to ensure more accurate WHOIS information and availability for Law Enforcement, in addition to improved transparency around domain name resellers and third party beneficiaries;

**WHEREAS** The G8 High Tech Crime Subgroup (HTCSG), which comprises representatives from law enforcement, justice departments and other governmental bodies of the G8 countries, is in support of these recommendations and recommends their implementation.

**WHEREAS** The following is a summary of due diligence recommendations for ICANN to adopt in accrediting registrars and registries and proposed amendments to the Registrar Accreditation Agreement (RAA), supported by the following international law enforcement agencies:

- Australian Federal Police;
- Department of Justice (US);
- Federal Bureau of Investigation (US);

- New Zealand Police;
- Royal Canadian Mounted Police;
- Serious Organised Crime Agency (UK)

The recommendations are considered to be required in order to aid the prevention and disruption of efforts to exploit domain registration procedures by criminal groups for criminal purposes. The proposed amendments take account of existing EU, US, Canadian and Australian legislation and their respective commitments to preserving the individual's rights to privacy.

### **1) Due Diligence**

- a. ICANN should perform due diligence investigations on all Registrars and Registries upon accreditation and periodically thereafter;
- b. The RAA should require Registrars to collect accurate and complete data of all Registrants upon domain name registration and periodically thereafter, in which the Registrar will validate to ensure such Registrant data is accurate and complete.

### **2) WHOIS Lookup & Domain Name Search**

In accordance with the ICANN's 2006 JPA Affirmation of Responsibilities, and the 2009 Affirmation of Commitments, all gTLD domain name WHOIS information must be accurate, detailed and public. Although LE does not support the use of proxy/privacy registrations, the LE agencies urge ICANN to exercise the following on proxy/privacy registrations:

- a. The proxy/privacy registrant is a private individual using the domain name for non-commercial purposes only, and ;
- b. The proxy/privacy registration service has been accredited by ICANN using the same due diligence process as a Registrar/Registry, and
- c. Information from the WHOIS database can be provided to law enforcement authorities when the information will assist in the prevention, detection, investigation prosecution or punishment of criminal offences or breaches of laws imposing penalties, or when authorised or required by law.

### **3) Transparency and Accountability**

- a. ICANN should require all domain name resellers and all third party beneficiaries to be held to the same terms and conditions and due diligence requirements as Registrars and Registries;

- b. ICANN should require all registrars, registries, proxy services, resellers and all third party beneficiaries of any contracts, policies of ICANN to publicly display ownership, parent companies, subsidiaries and business associations.

**WHEREAS** The international law enforcement community views the above-referenced recommendations as vital in preventing crimes involving the Domain Name System (DNS);

**WHEREAS** The law enforcement community has consulted with the Registrar and Registry community in preparing this document;

**WHEREAS** It is imperative that law enforcement and ICANN work together to ensure a safe and secure Internet.

**THEREFORE BE IT RESOLVED** that the Canadian Association of Chiefs of Police supports the above described due diligence recommendations to ensure a safe and secure Internet, and

**BE IT FURTHER RESOLVED** that the Executive of the Canadian Association of Chiefs of Police will send a letter of support of the above described due diligence recommendations to ICANN.

## **ACTIVITIES PLANNED/SIGNIFICANT DATES 2010/2011 :**

Winter 2010	Toronto, Committee Meeting January 21, 2010
Spring 2010	Halifax, Committee Meeting May 6/7, 2010
Summer 2010	Edmonton, In preparation for Annual CACP Meeting August 20/21, 2010
Winter 2011	Quebec, Committee Meeting January 12, 2011
Spring 2011	Ottawa, Committee Meeting (tentative) May 2011
Summer 2011	Annual CACP Meeting, Windsor, Ontario, August 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
- Analyse 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



## **COMMITTEE MEMBERS LIST:**

### **Tom Pownall**

Superintendent  
OIC - Technological Crime Branch  
RCMP Technical Operations  
St. Joseph Blvd.  
Ottawa, ON  
K1A0R2  
Telephone: (613) 998-6066  
Fax: (613) 993-2963  
Email: [tom.pownall@rcmp-grc.gc.ca](mailto:tom.pownall@rcmp-grc.gc.ca)



**Bio:** Supt Pownall joined the RCMP in 1985 and followed basic training with an assignment to the RCMP Federal Sections in Ottawa, Ontario. Following service in General Investigations Section and Traffic Section, he was transferred to Commercial Crime Section as a fraud investigator in 1988. In 1992 he was transferred to a position as a computer crime investigator with the Commercial Crime Section. Since that time he has held different positions in Technological Crime, including OIC - Policy and Program Management and he is currently the Officer-In-Charge of the national technological crime program. Supt Pownall currently represents the RCMP on the G8 High Tech Crime Working Group and the Strategic Alliance Cyber Crime Work Group.

Supt Pownall holds a Master of Business Administration from Concordia University, a Bachelor of Arts from McGill University and a Certificate of Management Practices from Concordia University. He also holds a Certificate in General Police Studies and Certificate in Advanced Police Studies from the Canadian Police College.

## **Ken MacKay**

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

## Dan Killam

Chief Superintendent  
Deputy Criminal Operations Officer  
Royal Canadian Mounted Police "K" Division  
Edmonton, Alberta  
T5G 2T4  
Telephone: (780) 412-5755  
Fax: (780) 412-5403  
Email: [dan.killam@rcmp-grc.gc.ca](mailto:dan.killam@rcmp-grc.gc.ca)



**Bio:** On July 21, 2008, Dan Killam became the Deputy Criminal Operations Officer - Integration and Intelligence, for RCMP "K" Division in Edmonton, Alberta. In this role, he is responsible for Major Crime investigations, National Security, Border Integrity, Immigration and Passport, Customs and Excise, Drug enforcement, Intelligence, Source Witness Protection and Protective Policing.

Chief Superintendent Killam is originally from Moncton, New Brunswick and has 34 years of service in a variety of policing duties within the RCMP.

Chief Superintendent Killam spent the first 11 years of his service in Alberta, working both in General Duty policing as well as carrying out plain clothes duties. His postings included: Sunde Detachment, Red Deer Detachment, Sylvan Lake Detachment, High Prairie Detachment and Red Deer Drug Section.

In 1987, Chief Superintendent Killam was transferred to the Special Emergency Response Team (SERT) in Ottawa, a full-time counter-terrorism team. After completing six years with SERT, Chief Superintendent Killam transferred to RCMP Headquarters in Ottawa where he worked Security Fraud and Computer Crime within the Economic Crime Directorate.

From 1994 until 1996, Chief Superintendent Killam was seconded to the Krever Commission of Inquiry into the Blood System in Canada to assist the inquiry in an investigative capacity. Following this posting, he accepted a two-year secondment to the Commission of Inquiry into the Deployment of Canadian Troops to Somalia in a similar role.

In 1998, Chief Superintendent Killam was seconded to the Department of National Defense (DND) to head up the Sensitive Investigation Section. This was a newly created unit within the Military Police National Investigation Section.

In June of 1999, Chief Superintendent Killam returned from his secondment to DND to assume responsibility for setting up and managing the RCMP's Critical Incident Program (CIP). The CIP is responsible for national coordination of RCMP negotiators, incident commanders, public order, Emergency Response Teams and Emergency Management resources.

In May 2002, Chief Superintendent Killam was transferred into the newly created position of Director General, Criminal Intelligence Support until June 2003, at which time he became the Director General National Security, Criminal Intelligence Directorate. He held this position until January of 2005 at which time he was transferred to "A" Division (National Capital Region - Ottawa) as the Officer-in-Charge of Criminal Investigations.

Chief Superintendent Killam received his Bachelor of Arts Degree from the University of Waterloo in 1993 and his Master of Public Administration Degree from Queen's University in 2001.

Chief Superintendent Killam presently resides in Edmonton, Alberta with his wife and daughter.

## 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](mailto: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.

## **Al Tario**

Inspector,  
Operations Support  
Criminal Investigation Service,  
Ottawa Police Service  
474 Elgin Street,  
Ottawa, Ontario  
K2P 2J6  
Telephone: (613) 236-1222 Ext: 5469  
Fax: (613) 760-8122  
Email: [tarioa@ottawapolice.ca](mailto:tarioa@ottawapolice.ca)



Bio: Inspector Al Tario has been a member of the Ottawa Police Service since 1980 and is presently the Officer in charge of Major Case Investigations in Criminal Investigations. The Units in this portfolio include; Major Crime, Cold Cases, Robbery, Partner Assault, Sexual Assault and Child Abuse, Elder Abuse and Hate Crimes.

Inspector Tario has been assigned to a number of areas of the police service in a variety of roles and ranks almost exclusively in an operational capacity, including, foot and car patrols, Tactical, Crime Prevention, Forensic Identification, General Assignment Investigations and Major Crime Investigations. At the rank of Inspector, Al has been assigned to the Duty Officer Program with responsibilities for Incident Command, as well as assignments as the OIC of the Tactical Unit and the Crisis Management Negotiation Unit, and he has also served as a Patrol Inspector in a Division. Inspector Tario was also previously responsible for Investigative Support Units within Criminal Investigations that include; High Tech Crime / Internet Child Exploitation and the Organized Fraud Section.

In 1999, Inspector Tario was the lead investigator assigned to the mass murder/suicide at the Ottawa Carleton Transit Commission and resulting lengthy Coroner's Inquest.

## 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](mailto: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.

## 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](mailto: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. Mr Charette assumed duties as OIC for a regional detachment in 2004 before being promoted Lieutenant 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.

Member of the LAES (Lawful Access Electronic Surveillance) subcommittee of the CACP since 2005, Mr.Charette assumed Co-chair duties of that committee in 2007. He is also member of the newly formed NTCAC (National Technological Crime Advisory Committee) subcommittee of the CACP.



## Ray Archer

Canadian Bankers Association  
888 Birchmount Rd., 6<sup>th</sup> Floor  
Scarborough, ON.  
M1K5L1

Telephone: (416)-615-4557  
Fax: (416) 615-5178  
Cell: (416) 371-5845  
Email: [ray.archer@scotiabank.com](mailto: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](mailto: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 for 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](mailto: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**

### **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](mailto:fthibode@cpc.gc.ca)



Canadian Police  
College  
Collège canadien  
de police

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](mailto: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.

## 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](mailto:GSansom@JUSTICE.GC.CA)



Department of Justice  
Canada

Ministère de la Justice  
Canada

**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**

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](mailto: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 panellist 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 in all levels of trial and appeal courts.

**Marc Moreau**

Staff Sergeant  
Technological Crime Branch  
i/c Policy & Standards  
1426 St-Joseph Blvd.,  
Ottawa, ON K1A 0R2  
Telephone: (613) 993-6011  
Fax: (613) 993-2963  
Email: [marc.moreau@rcmp-grc.gc.ca](mailto:marc.moreau@rcmp-grc.gc.ca)



**Bio:** S/Sgt Moreau is a member of the Royal Canadian Mounted Police with 30 years of service. He is currently responsible for Policy & Program Support of the National Technological Crime Program for the RCMP.

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 2008 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 involved in the on-going efforts to deliver an effective national enforcement program to conduct investigations in support of Canada's strategies to protect its national critical information infrastructure from the threats of natural disasters and terrorism.



## Appendix “A”



### **CACP E-crime Meeting January 7, 2010 Toronto, Ontario**

#### **Participating:**

Tom Pownall (Co-Chair)	RCMP - Ottawa
Kate Lines (Co-Chair)	OPP - Orillia
Martin Charette	Sûreté du Québec
Grant Foster	Saskatoon Police Service
Ken MacKay	Edmonton Police Service
Tom Fitzgerald	Toronto Police Service
Ray Archer	Canadian Bankers Association – Ontario
John Weigelt	Microsoft
Dan Rajsic	OPP – Orillia
Shawn Nash	OPP – Orillia
Marc Moreau	RCMP - Ottawa

#### **Participating via teleconference:**

Bessie Pang	Society for the Policing of Cyberspace
France Thibodeau	Canadian Police College
Alexander Smith	Attorney General, Crown Law Office – (Ont)

**Regrets:**

Al Tario, Ottawa,  
Peter Hourihan  
Gareth Samson  
Dan MacRury

Ottawa Police Service  
RCMP - Winnipeg  
Justice of Canada , Criminal Law Policy  
Nova Scotia – Public Prosecution Service

**1. Opening Remarks**

Co-Chairs Kate Lines and Tom Pownall brought the meeting to order and welcomed members.

**2. Minute of Silence**

In honour of Cst. Eric Czapnik, Ottawa Police Service who lost his life while performing his duties.

**3. Membership Issues**

The committee members acknowledged Supt. Grant Foster, Saskatoon Police and John Weigielt of Microsoft as new members of the CACP ECrime Committee and thanked them for his participation. The Committee would like to thank their predecessors, Supt Mark Chatterbok of the Saskatoon PS and Mr. Michael Eisen of Microsoft for their valued contribution to this Committee in the past.

The committee acknowledged the on-going lack of representation from the Maritime Provinces.

**4. Internet Governance (ICANN) – S/Sgt Marc Moreau (RCMP)**

Provided an overview of the Internet Corporation for Assigned Names and Numbers (ICANN) organization. The following is a description of ICANN obtained from their web site [www.icann.org](http://www.icann.org).

As a private-public partnership, ICANN is dedicated to preserving the operational stability of the Internet; to promoting competition; to achieving broad representation of global Internet communities; and to developing policy appropriate to its mission through bottom-up, consensus-based processes. ICANN, a public benefit, non-profit entity, is the international organization responsible for the management and oversight of the coordination of the Internets domain name system and its unique identifiers.

ICANN was created through a Memorandum of Understanding (MoU) between the U.S. Department of Commerce and ICANN to transition management of the Domain Name System (DNS) from the U.S. government to the global community. The most recently issued version of the MoU is intended to be the last and sets out a series of goals for ICANN that, when achieved, will result in a fully independent ICANN organization.

The RCMP along with the Sûreté du Québec has attended some of these meetings in the past. Any law enforcement agency is welcome to join our efforts at the international level.

The RCMP is also working with international law enforcement partners from the Strategic Alliance Group (SAG) that includes Australia, New Zealand, UK and the USA, to gain a voice in the governance of the Internet. This is in support of an international initiative called Project Minstrel. Co-Chair Tom Pownall is a member of the SAG.

The latest initiative from this group is the development of recommendations for ICANN consideration. A document entitled: "Law Enforcement Due Diligence Recommendations for ICANN" was distributed to E-Crime Committee members. It provides a summary of the following recommendations from law enforcement for ICANN to adopt:

- Due diligence
- WHOIS
- Transparency /Accountability

Marc Moreau further advises the RCMP also works closely with the FBI in ongoing efforts with ARIN (American Registry for Internet Numbers). In February 2009 the AGWG (ARIN/Government Working Group) was created. It brings together the ARIN and the law enforcement community to discuss matters of mutual concern. In attending the last meeting in October 2009 it was learned the International Telecommunication Union (ITU) has competing interest with ICANN in wanting to be recognized as a RIR (Regional Internet Registry). Failing this the ITU is believed to be looking at securing huge IPv6 internet block space. This may be of concern for law enforcement as it may prove difficult to obtain information from the ITU member countries. The concern is that ITU is essentially set up to be "top-down" type of organization. This means that certain countries would have more control to decide how the Internet service would be administered from one country to the next. On the other hand, ICANN is currently the authoritative governing agency that oversees the Internet management on a

world basis and it runs from a “bottom-up” governance approach. This assures an optimal level of transparency and complete consultation/canvassing of the various stakeholders that forms the international ICANN community. It is felt that law enforcement could face serious challenges with the former approach especially as it pertains to national security investigations. It is felt the ITU may not fully appreciate the risk that could develop if they were to turn over huge Internet block space to a country that may not look favorably in cooperating with law enforcement (or foreign government agencies). This could potentially have a negative impact on national security or critical information/infrastructure investigations.

Marc Moreau also provided an update with regards to CIRA (Canadian Internet Registration Authority), who manage the .CA domain in Canada. The RCMP worked closely with CIRA to develop a method that would allow the Canadian law enforcement community the opportunity to obtain WHOIS personal information of an individual in specific cases (ie: National Security, Child Exploitation, life at risk, etc). The Law Enforcement Request (LER) was introduced in June 2008 with the understanding there would be a further assessment in a year time. CIRA conducted a review of this practice during the summer months of 2009. The RCMP, OPP and the Sûreté du Québec each were contacted to provide feedback of this practice. The results of this consultation can be found at [www.cira.ca/whois](http://www.cira.ca/whois)

## **5. Review of Old Business**

Minutes of the last meeting accepted. Recommended by Martin Charette and seconded by John Weigelt.

Review of Committee correspondence. Kate Lines discussed correspondence between the committee and the CACP executive.

Update on communication with CACP executive regarding the CACP President's Council on Strategic Direction, January 17/18, 2010. Tom Pownall advises that Martin Charette will be attending this meeting on behalf of this Committee.

## **6. Bill C-46 Update**

Tom Pownall provided an overview of Bill C-46 regarding the status of Investigative Powers for the 21<sup>st</sup> Century Act.

## **7. Bill C-47 Update**

Tom Pownall provided an overview of Bill C-47 regarding Technical Assistance for law enforcement in the 21<sup>st</sup> Century Act.

## **8. Mobile Device Advancements – D/Sgt Kelly Anderson )OPP**

Kelly provided a good understanding of the history of the cellular telephone and its evolution. He also provided several examples of the level of details contained within a cellular and how its relevance in police investigations. Kelly also provided some examples of the evolution of technology in this field. For example there is the Mobile Spy that allows for the recording of SMS text messages and call info of a user. Tips and tricks were also provided on how to protect your cell phone. In closing Kelly also spoke about what the future may look like. For example the convergence and integration of technology is only limited by imagination. The reliance on cloud computing will be an interesting one to follow as concerns with regards to where the data will be stored and exactly who will have access will be of interest to the law enforcement community.

## **9. Economic Impact of Cyber Security – John Weigelt (Microsoft)**

John spoke about the economic impact of technology in today's society. He spoke about examples of how technology is pervasive in many aspects of the economy. According to Industry Canada, the successful integration of e-business into the Canadian economy is dependent upon the level of trust and confidence businesses and consumers have in the digital environment. The digital economy is an extension is the integration of e-business in the Canadian economy. It is believed that cloud computing and the global Internet hold tremendous promise for the digital economy. Cyber security is a cornerstone for the digital economy which along public safety and national security motivates industry and governments to work together to address the current challenges. (A copy of the presentation was attached in the distribution of these Minutes)

## **10. Update on PolCyb Activities in 2010 – Bessie Pang (PolCyb)**

### ***Potential Collaboration among E-Crime Committee, POLCYB, & SFU International Cybercrime Research Centre (ICRC):***

Bessie Pang advised that she has received Dan Rasjic's list of potential research topics for POLCYB and ICRC to explore opportunities for collaborative research. Dan advised the group of the topics he has listed. Bessie advised that Dan has requested for some preliminary information on legal and policy framework in other countries on Encryption in preparation for a FTP meeting in February. She has already provided Dan with the related resources for his reference.

Tom to seek advice from the CACP Executives about the possibility of developing an MOU regarding research collaboration with POLCYB & SFU. E-Crime Committee will engage in further discussions to determine the proposed research topic. Bessie advised that the MOU should be addressed jointly to herself as the "Associate Director, Programmes, ICRC" and Dr. Bill Glackman, Director, ICRC.

### ***Upcoming events:***

- POLCYB International Conference 2010, Burbank, C.A., May 12th & 13th, co-host: Walt Disney Co. [http://www.polcyb.org/conf2010/conf\\_2010.html](http://www.polcyb.org/conf2010/conf_2010.html)
- Annual POLCYB International Summit 2010, Kuala Lumpur, Malaysia - 4-day event (Dates: TBA - either Oct. 25th to 28th, or Nov. 15th to 18th), co-host: CyberSecurity Malaysia [http://www.polcyb.org/summit\\_2010/summit\\_2010.html](http://www.polcyb.org/summit_2010/summit_2010.html) - POLCYB would like to invite a representative from E-Crime Committee to present on the work of the committee. Travel expenses will be sponsored by Summit.

## **11. Review of the National Tech Crime Advisory Committee – S/Sgt Dan Rajsic (OPP)**

The following points regarding the CACP goals were discussed:

- CACP Strategic Plan
- Bill C-46 and C-47
- Forensic Processing - FastScan
- Virtual training
- Outsourcing of forensic request for service
- Succession planning for the Board
- Use of Civilians as forensic examiners

- Disclosure challenges
- FPT Working Group update
- Understudy – revisited
- Presentation by Il Kim, Sûreté du Québec regarding DVR extraction

### **12. 2010 Winter Olympics (and Other Major Events) – Supt . Tom Pownall (RCMP)**

Tom provided an update on resources that will be available during the Winter Olympics. He advises the RCMP has also identified resources for the upcoming G8 and G20 meetings in June 2010. Ray Archer advises that he may be called if additional resources are needed for financial cyber crimes. The OPP, Sûreté du Québec and the Edmonton PS all have offered their support to the RCMP in the event of a cyber incident during the Winter Olympics.

### **13. New Business/New Resolution/Next Steps – Co-Chairs**

Tom Pownall provided an update to Committee members regarding the National Cyber Security Strategy lead by Public Safety. The RCMP along with other federal agencies are working together to develop this important strategy. Additional funding and resources is anticipated from the federal government.

Tom Pownall and Marc Moreau will report back to the Committee by the next meeting with suggestions for new Resolutions for 2010.

## Appendix “B”



### **CACP E-crime Meeting May 6/7, 2010 Halifax, Nova Scotia**

#### **Participating:**

Tom Pownall (Co-Chair)	RCMP - Ottawa
Martin Charette	Sûreté du Québec
Gareth Sansom	Justice of Canada , Criminal Law Policy
Dan Killam	RCMP, Edmonton
Shawn Nash	OPP – Orillia
Grant Foster	Saskatoon Police Service
John Weigelt	Microsoft
Marc Moreau	RCMP - Ottawa

#### **Participating via teleconference:**

Bessie Pang	Society for the Policing of Cyberspace
-------------	--

#### **Regrets:**

Kate Lines (Co-Chair)	OPP - Orillia
Ken MacKay	Edmonton Police Service
Tom Fitzgerald	Toronto Police Service
Ray Archer	Canadian Bankers Association – Ontario
Al Tario, Ottawa,	Ottawa Police Service
Dan MacRury	Nova Scotia – Public Prosecution Service



**1. Opening Remarks and old business**

Co-Chair Tom Pownall brought the meeting to order and welcomed members. Acceptance of the Minutes of the January meeting. Recommended by Dan Killam and seconded by Martin Charrette.

**2. Membership Issues**

The committee acknowledged the on-going lack of representation from the Maritime provinces.

**3. Site Visit -**

Hosted by Kevin Mallay, NCO i/c Atlantic Regional Integrated Technological Crime Unit

The Committee visited the offices of the RCMP Atlantic Regional Integrated Technological Crime Unit (ARITCU) and Kevin Mallay provided a presentation on the digital forensic methodology, disclosure and report writing.

**4. Simon Fraser University and POLCYB**

Bessie Pang of POLCYB advises that POLCYB has terminated all dealings with SFU Cyber Crime Research Centre as of February 15, 2010. POLCYB has vacated the premises. Ms. Pang indicated that there were concerns in relation to unresolved issues. In view of the current managerial and personnel issues, Ms. Pang suggested that the committee not proceed with the R & D proposal at this time.

**5. Internet Governance (ICANN) – Due Diligence Recommendations**

Discussion. The RCMP is working with international law enforcement partners from the Strategic Alliance Group (SAG) that includes Australia, New Zealand, the UK and the USA, to gain a voice in the governance of the Internet. This is in support of an international initiative called Project Minstrel. Co-chair Tom Pownall is a member of the SAG.

The latest initiative from this group is the development of due diligence recommendations for ICANN consideration. A document entitled: "Law Enforcement Due Diligence Recommendations for ICANN" was distributed to E-Crime Committee members. It provides a summary of recommendations from law enforcement for ICANN to adopt.

It was proposed that a CACP resolution be put forward at the annual conference to suggest that the CACP endorse the recommendations and the CACP Executive provide a letter of written support to ICANN.

John Weigelt will consult within Microsoft to determine whether Microsoft will also provide a letter of written support to ICANN.

#### **6. National Tech Crime Advisory Committee - Legislative initiatives & concerns**

Martin Charette provided an update from the National Tech Crime Advisory Committee indicating that NTAC members are concerned with the lack of progress in regard to lawful access legislation and Investigative Powers for the 21<sup>st</sup> Century. He also advised that NTAC have concerns that the Intercept definition requires clarification. The NTAC meeting also raised concerns with respect to concerns with Bill C-131 (Section 184.4), as after May 8 the law may become unconstitutional in BC. NTAC also identified concerns with regard to the technical and legal challenges associated with Pre-paid cellular telephones.

#### **7. CERT Virtual training**

Tom Pownall described the CERT Virtual Training Environment that is available for law enforcement personnel. LE personnel with an Internet connection and a web browser may access high quality information security, computer forensics and incident response training. Additional information is available at [www.cert.org](http://www.cert.org).

#### **8. Validation of specialized technical tools**

Tom Pownall led a discussion of validation and described the RCMP validation program in the RCMP Technological Crime Branch. It was suggested that further work and analysis is required within NTAC prior to developing a formal CACP resolution to address the validation issues.

John Weigelt advised that Microsoft uses an established system in matters related to validation, common criteria, standards and guidelines. It was suggested that Microsoft personnel meet with Gord Hama, OIC – RCMP Validation Team to discuss applicability to law enforcement. Martin Charette confirmed that NTAC would be doing further work in relation to validation.

## **9. Fastscan**

Shawn Nash provided a presentation and led a discussion in relation to OPP use of Fast Scan. This software is used in specific and limited circumstances to get past forensic delays and categorize images. The product is free with the training program and works in both the Mac and Windows environment. The product meets reporting requirements for some Crown Attorneys office, but it is not clear what evidence is being missed.

Advantages include: use by ICE investigators; no need for computer forensic training, immediate comparison of images against a known data base of child pornography images; and quick report to Crown Attorneys for bail purposes.

Disadvantages include: the product has not been validated; police do not control the “known” database; the database is in the US; does not look at deleted data; does not pull from compressed files; evidentiary data may not be examined; issues around use for consent searches and the need for proper digital forensics under the authority of a warrant.

## **10. Virtual Worlds and Crime**

Gareth Sansom provided a presentation and led a discussion on virtual worlds and the opportunities for criminal activity. A copy of the presentation will be appended to the Minutes to describe crime in virtual worlds in relation to fraud, identity theft, theft of intellectual property, money laundering, extortion, child exploitation, botnets, terrorist activities (i.e. propaganda, planning, financing, and recruiting). Interpol has produced an informative report in relation to crime in virtual worlds.

### **11. Criminal Use of the Domain Name System (DNS)**

Gareth Sansom provided a presentation and led a discussion on criminal use of the DNS in relation to cache poisoning, domain hijacking, cyber squatting, typosquatting and fast flux hosting. Mr. Sansom stated that work in an international anti-phishing work group indicates that they will be moving toward the use of the IODEF extensions.

### **12. New Business/New Resolution/Next Steps**

- Tom Pownall stated that the next meeting would take place in Edmonton in advance of the CACP Annual Conference. A writing team of volunteers from the committee will meet on August 20<sup>th</sup> to prepare the draft annual report. The committee will meet on August 21<sup>st</sup> to review the draft annual report and approve the final report for submission to the CACP Executive.
- Tom Pownall and Marc Moreau agreed to prepare and distribute a draft resolution in relation to the Due Diligence recommendations to ICANN for review by committee members.