



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.

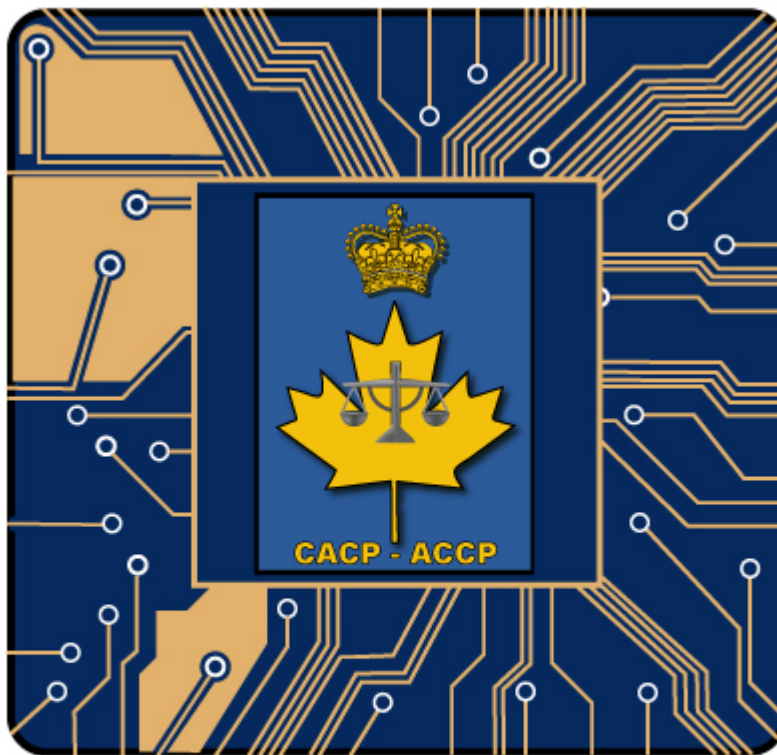
Certains de ces documents ne sont disponibles que dans une langue officielle. Sécurité publique Canada fournira une traduction sur demande.

**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 Annual Report



CACP e-Crime Committee

Table of Contents

Table of Contents	2
Annual Report	3
Message from the Chair	3
Committee Mandate/Objective	6
Resolutions.....	9
Preservation Order Commentary	9
Theft of Data Commentary	9
Resolution on the Preservation of Data	10
Resolution on the Theft of Data.....	11
Committee Members List:	13
CHAIRPERSON.....	13
CO-CHAIRPERSON	14
MEMBERS	15
A.J. (Tony) Warr.....	15
Paul McGrath.....	16
Bessie Pang	16
Peter MacAulay	17
Dan MacRury.....	17
Associate Corporate Member	18
Alec Taylor	18
Technical Advisors	19
Scott C. Hutchison	19
Susheel Gupta	19
Arni Stinnissen.....	20

Annual Report

MESSAGE FROM THE CHAIR

In March 2002 I wrote a memo that was eventually tabled with the CACP Board of Directors of the CACP proposing the establishment of an Electronic Crime (e-Crime) Committee. The mandate of this Committee would be to establish a CACP leadership role in the development of administrative policy and standards for technology-based investigations, the promotion of inter-agency cooperation in the detection and investigation of internet-based crime, the establishment of training standards and the identification of effective cooperative strategies to combat e-Crime at a local, Provincial, Canadian and International level. The e-Crime Committee was approved as a Standing Committee of the CACP and I was pleased to be asked to Chair this Committee. I am very pleased to have Assistant Commissioner Earl Moulton from the RCMP as Co-Chair. He not only brings a wealth of subject matter expertise to the Committee, he has also chaired the Policing for the Society of Cyberspace, (POLCYB) and has already established some significant public and private contacts/partners.

Since then the mandate has been expanded to include the facilitation of public education on information security.

The use of computers has risen drastically since 1994, and in the year 2000, 53% of Canadian citizens over the age of 15 reported using the Internet, with Ontario residents having the highest usage. Police agencies continue to witness an increase in the use of computer technology connected to the commission of criminal offences including homicide, criminal harassment, threatening, fraud and mischief. Organized criminal groups are now on-line conspiring with each other, and using the Internet and e-mail to carry out their criminal acts. As the use of computers continues to increase in society, so will the use of them by organized crime and thereby so will the victimization of Canada's citizens.

Computers and the Internet are becoming entrenched as a normal part of criminal investigations throughout Ontario and the rest of Canada. This area continues to be an evolving area of law, with little case law for guidance and best practices being implemented by individual police services.

It has become apparent that there is a lack of a coordinated effort in Canada to address these often-borderless crimes, which has adversely affected the ability of the police to gather evidence and investigate e-Crime. Criminals take advantage of cross-jurisdictional issues and the lack of global best practices in regards to digital evidence. Canadian police agencies such as Vancouver, Calgary, Edmonton, Winnipeg, Montreal, Ottawa and Quebec City and the RCMP have established computer crime units, and are developing their own policies and procedures for gathering electronic evidence. In Ontario the OPP, Ottawa and Peel Police have dedicated multi-person units for the investigation of electronic crime. Other Ontario police agencies such as Durham, York, Halton and Hamilton have one- or two-person teams.

Police agencies that do not have the resources to investigate e-Crime are left to ‘shop’ for an agency that will assist them in a technology-based investigation. A harmonized approach will minimize the creation of bad case law and project Canada as a world leader in e-Crime investigations. This approach will also smooth the process of national and international investigations.

The CACP once again is assuming a leadership role in addressing a serious challenge for policing that perhaps might be the biggest challenge policing has yet to face.

The CACP e-Crime Committee will have strong links to other CACP committees such as:

Community Policing and Crime Prevention Committee

- Knowledge of computers and the Internet is not equal amongst the police and citizens especially on crime prevention techniques, ethical issues and self-protection.

Law Amendments Committee

- Interpol, G8 group of countries, and the Federal/Provincial/Territorial Working Group on Cyber crime are meeting separately and jointly to discuss legislation amendments that will impact on every police jurisdiction in Canada.

Organized Crime Committee

- Organized crime is a business with technology and computers at the heart of their operations to compile counter-intelligence information and communicate anonymously with impunity. Almost all organized crime investigations involve an e-Crime component, which adds to the complexities that these investigations entail.

Police Information and Statistics Committee

- The POLIS committee is currently soliciting information on the definition of Internet Crime and the gathering of statistics for the Canadian Centre for Justice Statistics. There will be a demand for Internet crime data from academics, government policy makers, legislators, media and the public, to name a few.

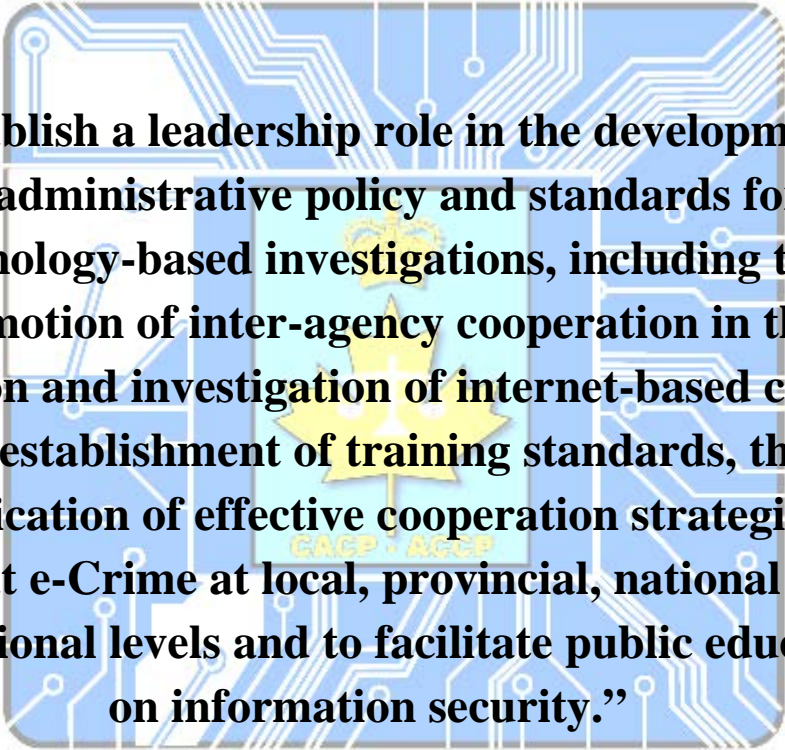
Prevention of Crime in Industry

- Software theft and piracy is a growing problem for high-tech industries

The electronic age is racing ahead, and Canada’s police must stay abreast to provide the best possible service to the community. Although a membership recruitment strategy for this Committee is still underway I can attest to the current membership as being leaders in the struggle to stay ahead of e-Crime issues.

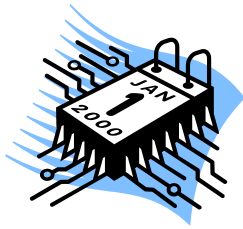
Canada's police services must meet the challenge to stay ahead of Electronic Crime challenges and this is an excellent opportunity, through this Committee, for the CACP to fill a definite void in knowledge and strategies to combat e-Crime.

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 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 to facilitate public education on information security.”

CACP e-Crime Committee



DATES/OVERVIEW OF MEETINGS

November 3, 2002

The inaugural meeting of the e-Crime Committee was held on November 3, 2002 at the Executive Airport Plaza Hotel & Conference Centre, Richmond, British Columbia. In attendance were:

Frank Ryder (Co-Chair)	OPP
Earl Moulton (Co-Chair)	RCMP
Bessie Pang	POLCYB
Peter MacAulay	RCMP

Items discussed included e-Crime Committee membership, frequency of meetings, communications and e-Crime Committee mandate.

July 4th, 2003

The second meeting of the e-Crime Committee was held by teleconference on July 4, 2003. Members participating included:

Frank Ryder (Co-Chair)	OPP
Earl Moulton (Co-Chair)	RCMP
Bessie Pang	POLCYB
Peter MacAulay	RCMP
Susheel Gupta	Justice Canada
Scott Hutchinson	Ministry of Attorney General (Ontario)
Ruth Sutton	BMO Financial Group

Arni Stinnissen	OPP – e-Crime Committee, Technical advisor
-----------------	--

Items discussed included new members and recruitment, the upcoming conference, Amendment to the e-Crime Committee Mandate, future meetings, resolutions, strategic plan, and the National Plan on the Exploitation of Children.



SUMMARY OF INITIATIVES/ACTIVITIES 2002/2003:

- Proposal was submitted to the CACP Board of Governors for their approval and a Standing Electronics Crime Committee was approved.
- Co-Chair identified
- Committee Mandate amended to include “facilitate public education on information security.”
- New members recruited from corporate and judicial sectors
- Strategy developed to staff committee
- Resolutions on ‘Theft of data’ and ‘ Preservation of Data’ drafted and submitted
- Meetings held to further linkages
- Initial discussions on National Strategy on Child Exploitation
- Initial discussions on Certification

RESOLUTIONS

The e-Crime Committee has submitted the following resolutions for consideration:

PRESERVATION ORDER COMMENTARY

The Council of Europe *Convention on Cyber-Crime* is an international treaty that provides signatory states with legal tools to help in the investigation and prosecution of computer crime, including Internet-based crime, and crime involving electronic evidence. As a permanent observer to the Council of Europe, Canada was invited to participate in the negotiation of the *Convention*. As of August 2002, 33 countries had signed the *Convention*, including Canada and most of its G8 partners. The *Convention* calls for the criminalization of certain offences relating to computers, the adoption of procedural powers in order to investigate and prosecute cyber-crime, and the promotion of international cooperation through mutual legal assistance and extradition in a criminal realm that knows no borders. A procedural mechanism in the Council of Europe *Convention on Cyber-Crime* that does not exist in Canadian law is the concept of a preservation order. A preservation order acts as an expedited judicial order that requires service providers, upon being served with the order, to store and save existing data that is specific to a transaction or client. The order is temporary, remaining in effect only as long as it takes law enforcement agencies to obtain a judicial warrant to seize the data or a production order to deliver the data. For example, a preservation order could require an Internet service provider (ISP) not to delete specific existing information relating to a specific subscriber. It is meant as a stopgap measure to ensure that information vital to a particular investigation is not deleted before law enforcement officials can obtain a search warrant or production order.

THEFT OF DATA COMMENTARY

Since the creation of information technology, digital information or data is used in the everyday lives of all Canadian citizens and businesses. Data is stored on a variety of media and is invisible to the naked eye and for all intents and purposes, intangible. The judgment of the Supreme Court of Canada in *R. v. Stewart*, [1988] 1 S.C.R. 963, holds that the offence of theft does not include the unauthorized acquisition of confidential information or data. Since that time, law enforcement and prosecutors have been unable to investigate the theft of data, as there was no federal statute that explicitly criminalized the unauthorized acquisition of confidential information and intellectual property. The economic losses associated with the unauthorized acquisition of confidential information including personal information and intellectual property can cause the ruination of a company and financial losses and great hardship to individual citizens.

The Economic Espionage Act, 1996, makes the theft or misappropriation of trade secrets a criminal offence, and is the first U.S. federal law that purports to both broadly define and severely punish such misappropriation and theft.

As more Canadians and Canadian enterprise conduct business on-line, data containing personal biographical information and corporate secrets become susceptible to unauthorized access by inside employees and attacks from the outside.

RESOLUTION ON THE PRESERVATION OF DATA

WHEREAS The Council of Europe *Convention on Cyber-Crime* is an international treaty that provides signatory states with legal tools to help in the investigation and prosecution of computer crime, including Internet-based crime, and crime involving electronic evidence;

WHEREAS Canada had signed the *Convention* which calls for the criminalization of certain offences relating to computers, the adoption of procedural powers in order to investigate and prosecute cyber-crime, and the promotion of international cooperation through mutual legal assistance and extradition in a criminal realm that knows no borders;

WHEREAS A procedural mechanism in the Council of Europe *Convention on Cyber-Crime* that does not exist in Canadian law is the concept of a preservation order;

WHEREAS Law enforcement requires the ability to obtain an order requiring the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification;

WHEREAS Law enforcement requires the ability through an order that requires the preservation of specified stored computer data in a person's possession or control. Legislation must be able to instruct the person to preserve the data and maintain the integrity of the data for a period of time as long as necessary up to a period of ninety days to enable law enforcement to seek its disclosure;

WHEREAS Preserved traffic data should be made available regardless of whether one or more service providers are involved in the transmission of that communication. Preserved traffic data should be disclosed to law enforcement or a person designated by that authority, of a sufficient amount of traffic data to enable law enforcement to identify the service providers and the path through which the communication was transmitted;

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police calls upon the Government of Canada through the Minister of the Solicitor General, the Minister of Justice and Attorney-General to amend the Criminal Code to create an order for the preservation of data in any form.

RESOLUTION ON THE THEFT OF DATA

WHEREAS the proliferation of information technology and the widespread use of the Internet have greatly enhanced the ability of unauthorized persons to acquire, without permission or colour of right, sensitive, confidential information and intellectual property;

WHEREAS the judgment of the Supreme Court of Canada in *R. v. Stewart*, [1988] 1 S.C.R. 963, holds that the offence of theft does not include the unauthorized acquisition of confidential information or data;

WHEREAS the limited sanction provided by s. 17 of the Copyright Act fails to properly address the societal harm associated with the unauthorized acquisition of confidential information and intellectual property.

WHEREAS the economic losses associated with the unauthorized acquisition of confidential information and intellectual property can cause the ruination of a company and financial losses and great hardship to individual citizens.

WHEREAS the recognition of the increasingly important role that confidential information and intellectual property plays in the well being of Canadian economy must include proper, comprehensive legal protection for such data.

WHEREAS the United States of America, and other jurisdictions, have legislation in place for protection from economic espionage, and the protection of trade secrets, and intellectual property

WHEREAS there is currently is no legislation that addresses the theft of data or intellectual property.

WHEREAS cases of ‘theft of data’ must be prosecuted as fraud and the prosecution is thereby obliged to establish economic deprivation and as such many cases of wrongdoing escape any sanction

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police calls upon the Government of Canada through the Minister of the Solicitor General, the Minister of Justice and Attorney-General to amend the Criminal Code to create an offence of unauthorized acquisition or theft of confidential information or data in any form.



ACTIVITIES PLANNED/SIGNIFICANT DATES:

August 24, 2003	Regular Committee Meeting Halifax, Nova Scotia
Nov 22-23, 2003	Fall Meeting, Montreal, PQ
TBD	Spring Meeting, Ottawa, ON
August, 2004	Regular Committee Meeting Vancouver, B.C.

Canada's police services must meet the challenge to stay ahead of Electronic Crime challenges and this is an excellent opportunity, through this Committee, for the CACP to fill a definite void in knowledge and strategies to combat e-Crime.

The challenge of the e-Crime Committee is to create a definitive strategic plan on how best to fulfill its mandate due to the multifaceted area of e-Crime. Most, if not all Canadian Police agencies subscribe to the definition of cyber crime as "a criminal offence involving a computer as the object of a crime, or the tool used to commit a material component of the offence." As indicated in the document created by Statistics Canada, "*Cyber Crime: Issues, Data Sources, and the Feasibility of the Collection Police-Reported Statistics*", there is also "computer-supported crime" which covers the use of computers by criminals for communication and document and data storage.

Over the course of the next few meetings, **The e-Crime Strategic Plan, A Foundation for Performance Measurement** will be created to properly guide the committee.

COMMITTEE MEMBERS LIST:

CHAIRPERSON

Frank Ryder

Chief Superintendent
Ontario Provincial Police
777 Memorial Avenue
Orillia, ON L3V 7V3
Phone: (705) 329-6315
Fax: (705) 329-6318
Email: frank.ryder@jus.gov.on.ca



Bio: Detective Chief Superintendent Frank Ryder leads Investigation Support Bureau of the Ontario Provincial Police. One of the Sections of his Bureau is e-Crime Section which has the mandate to provide specialized investigative services to OPP Regions, Detachments, Bureaux, Ontario municipal police services and government ministries facing investigations in which electronic equipment, and/or the Internet are identified as key elements of the investigation.

Detective Chief Superintendent Ryder has had a long affiliation with the Canadian Association of Chiefs of Police (CACP). In 1997 he became a member of the CACP by joining the Police Information and Statistics Committee (POLIS) and in 2000 he was appointed Co-Chair of this Committee a position he held for two years. In his capacity as Co-Chair of the POLIS Committee he also represented the CACP on two other committees: the Liaison Officers Committee (LOC) and the Police Advisory Committee Technical Advisory Committee (PACTAD).

In 2001, Detective Chief Superintendent Ryder left POLIS to become a member of the Law Amendments Committee (LAC), a position he still holds. In support of this Committee he also is a member of the CACP Resolutions Committee, which oversees resolutions presented to the CACP general membership on behalf of the CACP Board of Directors.

In 2002, he was mandated to lead the e-Crime Committee as one of the initial Co-Chairs.

CO-CHAIRPERSON

Earl Moulton

Assistant Commissioner
Commanding Officer, “F” Division
RCMP, Saskatchewan
6101 Dewdney Avenue,
Regina, SK S4P 3K7
Phone: (306) 780-5477
Fax: (306) 780-6966
Email: Earl.Moulton@rcmp-grc.gc.ca



Bio: Assistant Commissioner Moulton has been a member of the Royal Canadian Mounted Police for 25 years. Those years have seen duties ranging from policing remote First Nations communities in Saskatchewan to leading the Vancouver, British Columbia office of the RCMP’s Commercial Crime Section for four years. Assistant Commissioner Moulton was most recently responsible for the delivery of police services for most of the province of British Columbia, commanding a police force of 4100 sworn police officers. He has recently been promoted to the rank of Assistant Commissioner and taken command of policing services for the province of Saskatchewan.

Assistant Commissioner Moulton is also the founder and current President of the Society for the Policing of Cyberspace. That society is responsible for holding annual conferences and facilitating other international efforts to advance public safety in cyberspace. Integral to those efforts is increasing the cooperation between traditional police forces and their private industry counterparts.

In addition to his interests in general policing and cyberspace, Assistant Commissioner Moulton is an avid outdoorsman, canoeist and hockey player. He is married and father to two grown sons.

MEMBERS

Ruth Sutton

Bank of Montreal
Senior Manager-Security Operations
4100 Gordon Baker Road,
Scarborough, ON M1W 3E8
Phone: (416) 502-7274
Fax: (416) 502-5779
Email: ruth.Sutton@bmo.com



Bio: Ms. Sutton joined the Bank of Montreal Information Security Department in 2002 as DM/Senior Manager, Security Operations, managing a staff of 60 IT Security Specialists in Canada and the USA, out of the Toronto office. Reporting to the VP/CISO, she is accountable for managing a multi-million dollar budget, providing “active Security”, 7/24 through trusted, managed security services and the Information Protection Centre for intrusion monitoring, incidence response, etc. Ms. Sutton has enterprise accountability, providing security for BMO Group of Companies, Harris Bank, Nesbitt Burns, etc in twelve countries. Prior to joining BMO, served as the Director, Fraud and Security Risk Mgmt for CIBC’s Card Products division and served on numerous Risk Advisor Boards/Committees for the Canadian Banking Association, VISA, the International Association of Credit Card Investigators, CACP, etc. and is a past member of IACP/CACP from 1982-2001. Ms. Sutton has worked in the financial services industry in Security/Risk Management for 28 years. Ms. Sutton holds a degree in Criminology from UofT and is a Certified Fraud Examiner. Born and raised in Toronto, she is married with a 12 year old son and a 14 year old daughter.

A.J. (Tony) Warr

Staff Inspector
Unit Commander – Intelligence Support
Toronto Police Service,
40 College Street,
Toronto, ON M5G2J3
Phone: (416) 808-3513
Fax: (416) 808-3502
Email: tony.warr@torontopolice.on.ca



Bio: Staff Inspector Warr joined the Toronto Police Service as a cadet in 1965 and became a constable in 1969. Staff Inspector Warr has extensive investigational experience spending over 20 years in Investigative Squads, such as Homicide, Sexual Assault & Hold Up Squad. Staff Inspector Warr also spent 2.5 years as Investigator with Ontario Fire Marshal office. He is the Unit Commander of Intelligence since March 1, 2001. He formed the Technological Crime sub-section within the Technical Support Section of Intelligence in January 2003. It is comprised of 10 investigators trained in Forensic Examination of computers.

Paul McGrath

Director
Canadian Bankers Association
Box 348, Commerce Court West
30th Floor
Toronto, ON M5L 1G2
Telephone: (416)-362-6093 x 207
Fax: (416)-362-0412
Cell: (647)-225-6093
Email: pmcgrath@cba.ca

Bio: Mr. McGrath is the Director of Security for the CBA and is former RCMP officer with the Commercial Crime Branch.



CANADIAN BANKERS ASSOCIATION
ASSOCIATION DES BANQUIERS CANADIENS

Building a Better Understanding / Pour mieux se comprendre

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
Cell: (604) 671-7689
Email: polcyb@telus.net



Ms. Pang 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, Ms. Pang 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, Ms. Pang 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, Ms. Pang 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.” Ms. Pang also has extensive experience in policy development; development of provincial and federal standards, including staff training and equity employment; programme development and evaluations – including programmes for youth gangs, community policing, and domestic violence.

Ms. Pang 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, Ms. Pang also is assuming the role of the Executive Director of POLCYB.

Peter MacAulay

Superintendent
Officer in Charge, Technological Crime Branch
RCMP Ottawa,
St. Joseph Blvd.
Ottawa, ON K1A0R2
Telephone: 613 993-1777
Fax: 613 993-2963
Email: peter.macaulay@rcmp-grc.gc.ca



Bio: Superintendent Macaulay is the officer in charge of the Technological Crime Branch. It provides services at the request of any Canadian police service or government agency or, in the case of Internet investigations, international agencies. These services include expertise in computer search, seizure, forensic analysis, and expert witness testimony in criminal court proceedings.

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.

Associate Corporate Member

Alec Taylor

Business Productivity Advisor
Microsoft Canada
1950 Meadowvale Blvd.,
Mississauga, ON, L5N 8L9
Telephone: 905-363-8505
Fax: 905-568-0154
Cell: 416-577-6830
Email: alect@microsoft.com



Bio: Alec Taylor is a business productivity advisor with Microsoft Canada's public sector team. His focus is public safety and justice. Alec is leading a number of projects in the area of public safety aimed at helping police services effectively use technology to support intelligence-based policing and combat computer facilitated crime.

These projects including linking disparate databases within and across police agencies to support integrated crime analysis, use of secure mobile and wireless devices to support field operations, working with computer forensic investigators to explore ways that Microsoft can better support their efforts, and the development of a child exploitation linkage and tracking system.

Before joining Microsoft Alec was co-leader of KPMG's public sector risk management practice. He was responsible for providing risk strategy consulting services to all levels of government including projects for the Ontario Ministry of Public Safety and Security and Solicitor General Canada to identify barriers to information sharing across criminal justice agencies.

Alec holds a Master's degree in Public Administration and Public Policy from the London School of Economics.

Technical Advisors

Scott C. Hutchison

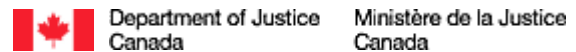
Crown Counsel,
Crown Law Office – Criminal (Ont.)
10th Floor, 720 Bay Street,
Toronto, Ontario, M5G 2K1
Phone: (416) 326-4585
Fax: (416) 326-4656
Email: scott.hutchison@jus.gov.on.ca



Bio: Scott C. Hutchison was called to the bar in Ontario in 1989 after serving as Law Clerk to the Ontario Court of Appeal. Since that time he has been employed as Crown Counsel, Crown Law Office – Criminal where he regularly appears in the Ontario Court of Appeal and Supreme Court of Canada on behalf of the Crown in criminal matters. From 1999 to 2002 he also served as Director for Law and Technology for the Criminal Law Division of the Ministry of the Attorney General. He is the author of a number of articles and texts on criminal law topics and frequently lectures on search and seizure law, as well as on the subject of computer crime.

Susheel Gupta

Federal Prosecutor/Computer Crime Advisor
Department of Justice Canada,
284 Wellington Street, EMB 2061,
Ottawa, ON, K1A 0H8
Telephone: (613)-941-8517 (24 hours)
Cell: (613)-941-8517
Email: sush@justice.gc.ca



Bio: Susheel Gupta is currently a Federal Prosecutor with the Department of Justice in Canada. Specifically, he has been designated the Computer Crime Advisor for the prosecution unit Ottawa. Sush is a Computer Crime Advisor who currently assists on prosecutions and investigations with the Federal, Provincial and Local governments and institutions. Sush is a director of POLCYB (The Society for the Policing of Cyberspace), publishes a daily Computer Crime Newsletter, and regularly instructs on the legal aspects of Cyber crime at the Canadian Police College. Sush is also a Training Coordinator for FPS on Computer Crime and works with the Department of Justice, the Federal/ Provincial/ Territorial Working Group on Cyber crime, and is a Canadian designate to task forces on Cyber crime with the FBI and the Secret Service. Sush is also an advocate for Internet Safety and presents many training sessions and presentations on the topic across Canada.

Arni Stinnissen

Detective Staff Sergeant
Manager- OPP e-Crime Section
777 Memorial Ave.,
Orillia, ON L3V 7V3
Phone: (705) 329-6441
Fax: (705) 329-6318
Email: Arni.Stinnissen@jus.gov.on.ca



Bio: Staff Sergeant Stinnissen is a senior police officer with over 25 years of experience with the Ontario Provincial Police. In years gone by, he worked in the Computer Services Branch of the OPP in Toronto where he was a systems officer providing maintenance on the Tandem mainframe system. He also provided help desk duties supporting the OPP's early growth in the computer area. Staff Sergeant Stinnissen was also project leader for the Anti-Rackets Section document imaging system.

Staff Sergeant Stinnissen is the Manager of the Electronic Crime Section, which handles reported computer-based crime for the OPP and other clients such as municipal police services and government agencies. Staff Sergeant Stinnissen is a regular speaker in the police community on topics such as search and seizure, electronic evidence and information age crime. Staff Sergeant Stinnissen has successfully completed numerous computer-based courses from the Canadian Police College and is a part-time professor at Georgian College for their Cyberspace Security Program. Staff Sergeant Stinnissen is also a member of the FPT/WG on Cyber crime.