



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.

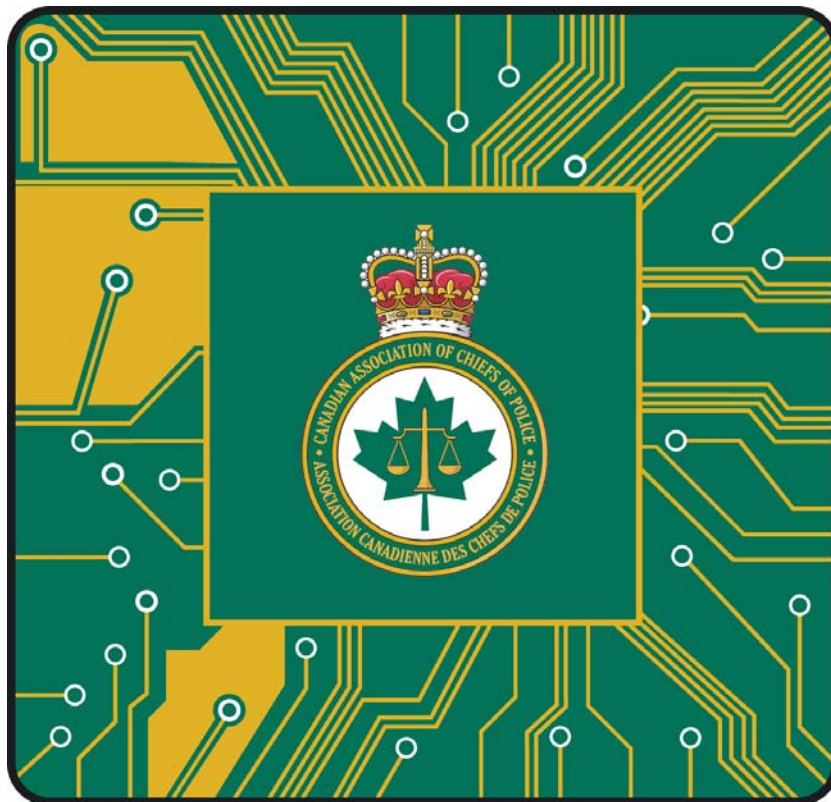
Some of these documents are available in only one official language. Translation, to be provided by Public Safety Canada, is available upon request.

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>Canadian Association of Chiefs of Police Leading Progressive Change in Policing</p>	 The logo of the Canadian Association of Chiefs of Police (CACCP) is circular, featuring a crown at the top, a central green maple leaf with a white scale of justice, and the text "CANADIAN ASSOCIATION OF CHIEFS OF POLICE" and "ASSOCIATION CANADIENNE DES CHIEFS DE POLICE" around the perimeter.	<p>L'Association canadienne des chefs de police À l'avant-garde du progrès policier</p>
---	---	--

Electronic Crime Committee 2009 Annual Report



CACP e-Crime Committee

TABLE OF CONTENTS

Table of Contents.....	2
2009 Message from the Chairs.....	3
Committee Mandate/Objective.....	5
Dates/Overview of Meetings.....	6
Summary of Initiatives/Activities 2008/2009:.....	10
Summary of Outstanding Resolutions from 2006 and 2007.....	11
Resolution 2007-06	11
Resolution 2007-07	13
Resolution 2006-08	16
Minimum Sentence for Luring Offences	16
Activities Planned/Significant Dates.....	18
Committee Members List:.....	19
CHAIRPERSONS	19
Kate Lines.....	19
Tom Pownall.....	20
MEMBERS	21
Peter Hourihan.....	22
Thomas Fitzgerald.....	23
Al Tario.....	24
Mark Chatterbok.....	25
Ray Archer.....	27
ASSOCIATE MEMBERS	28
Michael Kert Eisen.....	28
Bessie Pang.....	29
TECHNICAL ADVISORS	30
France Thibodeau.....	30
Susheel Gupta.....	31
Dan MacRury.....	32
Gareth Sansom.....	33
Alex Smith.....	34
Marc Moreau.....	35
Dan Rajsic.....	36
Appendix “A”.....	37
CACP e-Crime Committee January 21, 2009 – Vancouver, B.C.	37
Appendix “B”.....	45
CACP E-crime meeting June 4, 2009 Toronto, Ontario.....	45

2009 MESSAGE FROM THE CHAIRS

We are pleased to report on the 2008/2009 activities of the CACP E-Crime Committee. We continue to follow our Strategic Plan as it is our 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 work closely with other CACP Committees.

We have made efforts to establish membership enrolment that is truly national 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 E-Crime Committee held three meetings in the last year. A winter meeting was held in Vancouver in January and a spring meeting in was held in Toronto in June. The third meeting was held prior to the Annual CACP meeting in Charlottetown in August 2009.

Canada's Police Services must work together to address the many e-crime challenges. This Committee continues to be an excellent venue to share knowledge, skills and abilities, to augment current strategies in combating E-Crime. At the last year's annual CACP meeting in Montreal in August 2008, the E-Crime Committee received approval from CACP Executive to create a National Tech Crime Advisory Sub-Committee. The Sub-Committee now provides advice and guidance to the E-Crime Committee on technical, legislative and operational issues that impact technology based investigations. These meetings are held consecutively with other CACP sub-committee meetings to maximize participations and maximize cost savings.

This year, working with the support of the NTCAC, the Committee concluded the following work :

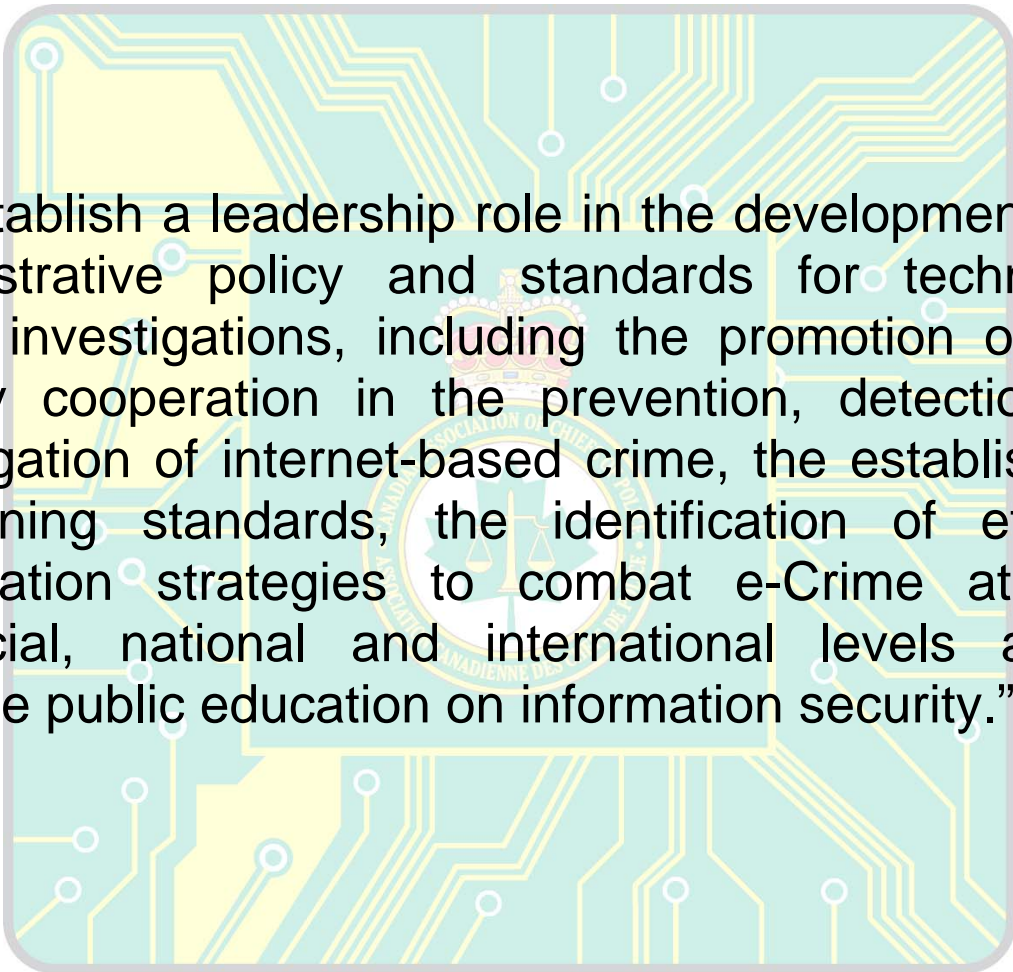
- Formalized agreement on core training courses required for technological crime forensic examiners to serve as a recommended national standard for the Canadian LE enforcement community. Committee members believe this recommended national standard for digital forensics is a first in the international law enforcement community
- A Recommended Guide for an Understudy Program for technological crime forensic investigators. This Guide incorporates the national training standard, practical work experience, demonstrated core competencies and continuous learning. This Understudy Guide is available to the broader law enforcement community to serve as a recommended model. This will prove valuable for any law enforcement agency looking to establish a Technological Crime program.
- The First Responders Best Practices for Digital Evidence. These Best Practices serve as a guide for Tech Crime forensic investigators. This Guide is available to Canadian law enforcement through the CACP web site
- A revised CACP E-Crime Committee Strategic Plan for the period 2009-2012. The Committee identified individual champions to lead each goal.

All three E-Crime Committee Resolutions remain outstanding. These Resolutions can be found starting on page 11 of this report

Chief Superintendent Kate Lines
Ontario Provincial Police

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 to 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 as well as expenses of ancillary expenses.

The winter 2009 meeting of the e-Crime Committee was held on January 21, 2009 at the Westin Hotel in Vancouver, British Columbia. In attendance were:

Winter 2009

Participating:

Tom Pownall (Co-Chair)	RCMP – Ottawa
Dick Bent	RCMP - Vancouver
Al Tario, Ottawa,	Ottawa Police Service
Mark Chatterbok	Saskatoon Police Service
France Thibodeau	Canadian Police College
Bessie Pang	Society for the Policing of Cyberspace
Marc Moreau	RCMP – Ottawa
Ken MacKay	Edmonton Police Service
Martin Charette	Sûreté du Québec

Participating via teleconference:

Kate Lines (Co-Chair)	OPP - Orillia
Dan Rajsic	OPP - Orillia

Regrets:

Ray Archer	Canadian Bankers Association – Ontario
Michael Eisen	Microsoft
Randy Robar	RCMP – Charlottetown
Alain Dubuc	Sûreté du Québec
Gareth Samson	Justice of Canada , Criminal Law Policy
Alexander Smith	Attorney General, Crown Law Office – (Ont)
Dan MacRury	Nova Scotia – Public Prosecution Service
Steve Izzett	Toronto Police Service

Items discussed included:

- Review of the final draft of the Best Practices for First Responders to Digital Evidence
- Role of the Committee in Internet Governance (ICANN/ NARALO/CIRA)
- Review of the final revised CACP E-Crimes Committee Strategic Plan
- PoICyb Activities in 2009
- Review of the National Tech Crime Advisory Committee (NTCAC)
- Review the status of outstanding Resolutions (2006-2007)
- E-Crimes Committee presence on CACP web site

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

Spring 2009

The spring 2009 meeting of the e-Crime Committee was held on June 4, 2009 at the Canadian Bankers Association, Toronto, Ontario. In attendance were:

Participating:

Tom Pownall (Co-Chair)	RCMP – Ottawa
Kate Lines (Co-Chair)	OPP - Orillia
Al Tario, Ottawa,	Ottawa Police Service
Mark Chatterbok	Saskatoon Police Service
Ken MacKay	Edmonton Police Service
Martin Charette	Sûreté du Québec
Tom Fitzgerald	Toronto Police Service
Ray Archer	Canadian Bankers Association – Ontario
Marc Moreau	RCMP – Ottawa
Dan Rajsic	OPP - Orillia

Participating via teleconference:

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

Regrets:

France Thibodeau	Canadian Police College
Michael Eisen	Microsoft
Randy Robar	RCMP – Charlottetown
Gareth Samson	Justice of Canada , Criminal Law Policy
Alexander Smith	Attorney General, Crown Law Office – (Ont)
Dan MacRury	Nova Scotia – Public Prosecution Service

Guests:

Peter Cuthbert – Executive Director, CACP
Det. Maureen Bryden – Ottawa Police Service

Items discussed included:

- Presentation by Det Maureen Bryden, Ottawa PS on Child Exploitation
 - Provincial and National Strategy
- CACP Update Provided by Peter Cuthbert, Executive Director, CACP
- Review of the National Tech Crime Advisory Committee (NTCAC)
- Role of the Committee in Internet Governance (ICANN/CIRA)
- Review of certain areas of the Strategic Plan
- PolCyb Activities in 2009
- Strategic Alliance Group (SAG) – Update

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

SUMMARY OF INITIATIVES/ACTIVITIES 2008/2009:

- Formalized agreement on core training courses required for technological crime forensic examiners to serve as a recommended national standard for the Canadian LE enforcement community.
- Developed and concluded a Recommended Guide for an Understudy Program for technological crime forensic investigators. This Guide incorporates the national training standard, practical work experience, demonstrated core competencies and continuous learning.
- Developed and finalized the First Responder Best Practices for Digital Evidence
- Revised the CACP E-Crime Committee Strategic Plan 2009-2012
- Identification of DVR (Digital Video Recorders) as an emerging risk area for law enforcement.

Summary of Outstanding Resolutions from 2006 and 2007

Resolution 2007-06

Lawful Access to Encrypted Electronic Media

Commentary

Sections 487 (2.1) and (2.2) provide law enforcement with access to data on computer systems which is described in the search warrant but there are now an increasing number of security features including encryption techniques available to computer systems to ensure that unauthorized users do not access data on computer systems. Criminal use of computer security technology such as passwords, encryption and other means, can result in situations where, during the execution of a lawful search, law enforcement is not able to access and interpret the data on a computer system described in the search warrant. The Criminal Code should be amended to require persons in control of a computer system and/or data to provide any and all computer passwords, encryption keys and other means, that secure data in a computer system during the execution of a search warrant.

Media Lines

- There are now an increasing number of security features including encryption techniques available to computer systems to ensure that unauthorized users do not access data on computer systems.
- Criminal use of computer security technology such as passwords, encryption and other means, can result in situations where, during the execution of a lawful search, law enforcement is not able to access and interpret the data on a computer system described in the search warrant.
- An encryption key itself would not likely be self-incriminating evidence as the use of it only allows access to previously inaccessible electronic information. It is information that will either exonerate or provide more evidence, which would be used to aid in determining guilt in a judicial proceeding.
- Law Enforcement choosing to use this avenue of investigative technique should have to provide reasonable and probable grounds sworn before the appropriate judicial official as to why they believe that evidence that they seek to investigate a serious crime cannot be accessed due to one or more encryption methods.

RESOLUTION

2007 -06

Lawful Access to Encrypted Electronic Media Commentary
Submitted by the e-Crime Committee

WHEREAS Sections 487 (2.1) and (2.2) provide law enforcement with access to data on computer systems which are described in a search warrant. There are now an increasing number of security features available to users of computer systems to ensure that unauthorized users do not access data on such computer systems. Criminal use of computer security technology such as passwords, encryption and other means, can result in situations where, during the execution of a lawful search, law enforcement is not able to access and interpret the data on a computer system or media described in the search warrant.

WHEREAS Section 487 (2.2) of the Criminal Code and Section 16 (2) of the Competition Act provide that "any person named in the warrant to use or cause to be used any computer system or part thereof on the premises to search any data contained in or available to the computer system for data from which a record that that person is authorized to search for may be produced", however the issue of encryption in relation to these sections has not been clarified by the courts but with some revised wording may provide some relief in this regard.

WHEREAS There are increasing instances of encryption being used to impede law enforcement. Encryption in its varying degrees has the potential to stop investigations. Data protected with properly implemented strong encryption technology continues to be very difficult, if not impossible, to decrypt unless one has access to the decryption key.

WHEREAS Section 341 of the Criminal Code already provides limited relief in this regard but the wording is non-specific and may be interpreted to include data but is restricted to "a fraudulent purpose" and omitting other serious offences.

WHEREAS Section 341 of the Criminal Code could be amended to include criminal purpose and include serious offences.

WHEREAS The most impenetrable physical structure can be opened with force, but not so in the virtual world. Reasonable and probable grounds to believe evidence exists is a core fundamental of Criminal Code Search warrants and this belief would have to justify access to encrypted files.

WHEREAS Provisions already exist in the Criminal Code of Canada that allow for suspects to provide potentially self-incriminating evidence such as breath samples, blood samples, DNA and fingerprints.

WHEREAS Provisions that already exist in the Criminal Code of Canada that demand potentially self-incriminating evidence also provide a penalty equivalent to the crime being investigated and should be included as a deterrent should the suspect contemplate not providing the encryption key.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police call upon the Government of Canada through the Minister of Justice and Attorney-General to amend the Criminal Code to provide a requirement which would compel any person who has care and control of electronic data contained in a computer system which is the subject of a lawful search, to provide any password or encryption key preventing access to that data by law enforcement, and;

BE IT FURTHER RESOLVED that the Canadian Association of Chiefs of Police call upon the Government of Canada through the Minister of Justice and Attorney-General to amend the Criminal Code of Canada so as to create an offence for failing to comply with an order to provide a password or encryption key as aforesaid, which offence would be punishable by the same penalty as the subject offence under investigation.

Resolution 2007-07

False Messages by Telecommunications also know as: Cyberthreatening, Cyberstalking, Cybermessaging

Commentary

Technology has changed how we communicate forever. Technology is ubiquitous in our everyday lives and has the ability to turn seemingly innocuous communications into weapons that have the power to intimidate, castigate and humiliate other citizens. Our youth in particular have embraced advanced means of sending messages. Further, due to generational gaps and differences in technical skills, today's youth are not always provided guidance in appropriate behaviours and potential risks when using technology. Cyberbullying is a term that is often used to describe this new phenomenon and the term 'bullying' brings a connotation that it is only a youth issue. Regrettably, however, adults are also using modern technology to terrorize, criticize and debase other citizens as well and are not leading by example. As a result, it is now common to experience or witness events of electronic telecommunications abuse or cyberbullying. Presently, law enforcement has very limited options when dealing with these issues in a criminal manner. Available measures at present include investigations of criminal harassment, threatening, defamatory libel, all of which carry heavy punitive consequences. The false messages section of the Criminal Code may provide the most likely criminal offence but each of the subsections offers restrictive and limited options and do not include present day technology. Each of the subsections also provide

differing penalties possibly restricting or impacting options on whether or not charges should be laid. Changes to Section 372 of the Criminal Code would provide law enforcement with new tools to address False Messages By Telecommunications by youth and other users of the Internet.

Media Lines

- Technology is present in all aspects of our everyday lives and has the power to turn seemingly innocuous communications into weapons that have the power to harm our citizens through acts of intimidation, humiliation and the like.
- Due to generational gaps and differences in technical skills, today's youth are not always provided guidance in appropriate behaviors and potential risks when using technology.
- It is now common to experience or witness events of electronic telecommunications abuse or cyberbullying. Presently law enforcement has very limited options when dealing with these issues in a criminal manner.
- The Canadian Government can be seen as providing a legislative solution to tackle changes in modern society and addressing public safety concerns that outdated legislation appears to have little deterrent.

Resolution

2007 - 07

Cyberthreatening, Cyberstalking, Cybermessaging
(False Messages by Telecommunications)
Submitted by the e-Crime Committee

WHEREAS Canadians have connected to the Internet and embraced computer related technologies at one of the highest rates in the world;

WHEREAS Electronic communications have too often been turned into weapons that have the power to intimidate, castigate and humiliate victims, and perpetrators are youth and adults alike;

WHEREAS A recent study (2007) conducted by Kids Help Phone has found that 70% of youth have been cyber-bullied and 53% of youth have been witness to cyberbullying events, and; _____

WHEREAS the same study conducted by Kids Help Phone found that 44% of youth suggested that there be zero tolerance and 41% believed that students should be punished;

WHEREAS Today's youth are not being properly guided in proper behaviors and potential risks when using technology due to generational gaps and differences in technical skills;

WHEREAS Cyberbullying is a term that is often used to describe this new phenomenon and the term 'bullying' brings a connotation that it is only a youth issue when in fact adults are using modern technology to terrorize, criticize and debase other citizens as well and are not leading by example;

WHEREAS Law enforcement has very limited options when dealing with false messages using modern telecommunications in a criminal manner. Present measures include investigations of criminal harassment, threatening, defamatory libel, all of which carry heavy punitive measures;

WHEREAS The Canadian Government can be seen as providing a legislative solution to tackle changes in modern society and respond to public safety concerns that outdated legislation appears unable to address;

WHEREAS An update to Section 372 of the Criminal Code False Messages would update the present wording to include modern communication methods including telecommunications;

WHEREAS an update to the penalty portion of Section 372 to make hybrid all three offences, currently, False Messages is a straight indictable offence (with a maximum penalty of two years), while the other two offences in s. 372 are straight summary offences;

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police calls upon the Government of Canada through the Minister of Justice and Attorney-General to amend Section 372 of the Criminal Code to provide for a modernization of wording so as to include telecommunications and to make hybrid each of the 3 related subsections to allow for maximum investigational and prosecution benefit.

Resolution 2006-08

Minimum Sentence for Luring Offences

Commentary

Bill C-2 constitutes the Government's response to a wide variety of recently articulated public concerns. Following Bill C-2 amendments, an adult's sexual contact with someone anyone over 14, but under 18 will also constitute an offence where the relationship is "exploitative of the young person." The maximum available penalty is increased from five to ten years' imprisonment and minimum penalties are imposed. At the same time, the maximum penalties for convictions under section 215 (failing to provide necessities of life) and section 218 (abandoning a child) are increased from two to five years. Bill C-2 does not address the offence of luring under s. 172.1(1) which is an obvious form of exploitation of children. However, many of the predicate offences involved in luring do now have mandatory minimum sentences.

Media Lines

- Bill C-2 constitutes the Government's response to a wide variety of recently articulated public concerns.
- The preamble to Bill C-2 recognizes that Canada has "grave concerns regarding the vulnerability of children to all forms of exploitation, including child pornography, sexual exploitation, abuse and neglect".
- The increased penalties noted above reflected that concern. For those offences where mandatory minimums were imposed, conditional sentences are no longer available
- The offence of luring under s. 172.1(1) is an obvious form of exploitation of children yet was not addressed in Bill C-2.
- The offence of luring is a serious form of child exploitation and the penalties should reflect the significance of the charge.

RESOLUTION 2006-08

Minimum Sentencing for Luring Section 172.1 (2) Criminal Code of Canada

Submitted by the e-Crime Committee

WHEREAS With the proclamation of Bill C-2 maximum penalties for offences involving the exploitation and abuse of children were increased and mandatory minimums imposed. The preamble to Bill C-2 recognizes that Canada has “grave concerns regarding the vulnerability of children to all forms of exploitation, including child pornography, sexual exploitation, abuse and neglect”. The increased penalties noted above reflected that concern. For those offences where mandatory minimums were imposed, conditional sentences are no longer available;

WHEREAS The offence of luring under s. 172.1(1) is an obvious form of exploitation of children yet was not addressed in Bill C-2. However, many of the predicate offences involved in luring do now have mandatory minimum sentences. As well, for those that are hybrid offences, most now carry a maximum summary penalty of eighteen months.

WHEREAS The offence of luring is a serious form of child exploitation and the penalties should reflect the significance of the charge. The same policy concerns which lead to the imposition for mandatory minimums and increased maximums in Bill C-2 are equally applicable to the offence of luring.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police calls upon the Government of Canada through the Minister of Justice and Attorney-General to amend the Criminal Code to Amend s. 172.1(2) (b) of the *Criminal Code* to provide for a maximum sentence of eighteen months for a summary offence; Amend s. 172.1(2) (a) and (b) to provide for mandatory minimum sentences of imprisonment.

ACTIVITIES PLANNED/SIGNIFICANT DATES

2009/2010 :

Winter 2009	British Columbia, Committee Meeting January 21, 2009
Spring 2009	Toronto, Committee Meeting June 4, 2009
Summer 2009	Committee Meeting for Annual CACP Meeting August 7, 2009
Winter 2010	Toronto, Committee Meeting (proposed) January 7, 2010
Spring 2010	Ottawa, Committee Meeting (proposed) May 2010
Summer 2010	Edmonton, August 2010

- 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
- Monitor development of the Cyber Crime Center of Excellence initiatives
- Identify opportunities for prevention and awareness
- Submission to CACP magazine
- Assess outstanding E-Crime Resolutions (2006-2007) in terms of new legislation, the Investigative Powers of the 21st Century (Bill C-46) and TALEA (Technical Assistance for Law Enforcement in the 21st Century (Bill C-47).
- Assess recruitment and retention issues for Tech Crime Programs

COMMITTEE MEMBERS LIST:

CHAIRPERSONS

Kate Lines

Chief Superintendent
Ontario Provincial Police
Investigation and Support Bureau
777 Memorial Avenue
Orillia, ON
L3V 7V3
Telephone: (705) 329-6315
Fax: (705) 329-6318
Email: Kate.Lines@ontario.ca



Bio: Chief Superintendent Kate Lines has been a member of the Ontario Provincial Police for 32 years.

She holds a Bachelor of Arts Degree majoring in Sociology in conjunction with the Crime and Deviance Specialist Program from the University of Toronto. She has also received General and Advanced Certificates in Police Studies and a Diploma in Police Management Studies from the University of Western Ontario.

C/Supt Lines has worked as a police officer in uniform, undercover drug investigations, fraud investigations, intelligence and major crimes such as homicide and sexual assault. She attended the FBI's Criminal Profiling Fellowship Program 1990-91 in Quantico, Virginia and was the second Canadian to graduate the program. She is also a graduate of the first Leadership in Counter Terrorism session.

C/Supt Lines is currently the Investigation and Support Bureau Commander responsible for the Criminal Investigation Services, Behavioural Sciences and Analysis Services and Forensic Identification and Technical Services Sections. She also oversees OPP's Investigations and Organized Crime Command Shared Administrative Services.

C/Supt Lines was voted Canadian Police Leader of the Year in 2004. She is also the recipient of the Officer Order of Merit Medal, Queen's Golden Jubilee Medal and the Ontario Provincial Police Exemplary Service Medal.

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



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.

MEMBERS

Ken MacKay

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



Ken MacKay is a 30 year member of the Edmonton Police Service currently in charge of the Specialized Investigations Division. This Division includes the Organized Crime Branch, the Investigative Support Branch, and the Intelligence Branch

Superintendent MacKay 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 as a Patrol Inspector, and then moved to the Corporate Planning Branch, before being promoted to Superintendent as the Executive Officer to the Chief of Police.

Ken has led or participated in a number of organizational wide change initiatives including the development and implementation of a new Family Division; two Organizational Reviews; project manager on the implementation of the new business intelligence tool; and recently assisting in the coordination and on-going implementation of Chief Boyd's 100 Day Plan.

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

Peter Hourihan

Chief Superintendent
Criminal Operations Officer
Royal Canadian Mounted Police "D" Division
Winnipeg, Manitoba
R3C 3K2
Telephone: (204) 984-6347
Fax: (204) 984-3637
Email: Peter.W.Hourihan@rcmp-grc.gc.ca



Bio: Chief Superintendent Peter Hourihan, originally from Alberta, joined the RCMP in September 1976. He has served in Saskatchewan, the Northwest Territories (now Nunavut), National Headquarters in Ottawa and for the past nine years, in Manitoba.. He has experience in General Duties, Traffic, Commercial Crime, Proceeds of Crime, Northern Policing and Corporate Management.

Peter was commissioned from Saskatoon Commercial Crime into the Integrated Proceeds of Crime Section in Winnipeg. He went from there to Client Services and in 2002 was promoted to Superintendent as the District Commander for the North District. In 2005, he was promoted to Chief Superintendent as the Corporate Management Officer for the Northwest Region.

Chief Superintendent Hourihan has a Bachelor's Degree in Business Administration from Athabasca University and a Bachelor of Laws from the University of Ottawa. He received the Long Service medal in 1996 and the Queen's Jubilee Medal in 2002.

Peter is married to Donna and they have two children, Chris (18) and Michelle (16).

Thomas Fitzgerald

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



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

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

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: tario@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 the Investigative Support Units in Criminal Investigations. These units include; High Tech Crime, Adult Missing Persons, Mental Health Crisis, Crime Stoppers, Harassing Phone Calls, Fraud, Auto Theft, Arson, Youth Intervention, Firearms, Guns and Gangs and Forensic Identification.

Al 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.

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

Mark Chatterbok

Detective Superintendent
Saskatoon Police Service
P.O. Box 1728
Saskatoon, SK.
S7K 3R6
Telephone: (306) 975-8343
Email: mark.chatterbok@police.saskatoon.sk.ca



Mark Chatterbok has been a member of the Saskatoon Police Service since December 1, 1981. He began his career as a Special Constable and in 1984 was hired as a regular Constable and attended the Saskatchewan Police College in Regina. Mark spent the majority of his early years working in Patrol, before working in the Traffic Section and Morality Section. In 2002 he was promoted to the rank of Sergeant and spent time in the Vice Unit and Training Section.

In 2005, Mark was promoted to the rank of Inspector and was in charge of the Human Resources Division, before being appointed as the Executive Officer to the Chief of Police. After one year in that position, he was assigned to the Records Management Division, in charge of Communications, Detention, Central Records and court operations. In January 2007, he was promoted to the rank of Detective Superintendent and is currently in charge of the Criminal Investigations Division.

Mark obtained an undergraduate and graduate degree from the University of Saskatchewan and is currently an Honorary Aide de Camp to the Lieutenant Governor of Saskatchewan. Detective Superintendent Chatterbok has attended several operational and administrative courses at the Canadian Police College, the Saskatchewan Police College and RCMP Depot. He has also participated on several local and provincial committees in relation to policing and has volunteered for various events in Saskatoon. Mark is the president of the Saskatoon Police Executive Officers' Association and is a trustee on the Saskatoon City Police Pension Plan.

Martin Charette

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



Bio: Martin 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. M. 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, M.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., 6th Floor
Scarborough, ON.
M1K5L1

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



CANADIAN BANKERS ASSOCIATION
ASSOCIATION DES BANQUIERS CANADIENS

Building a Better Understanding / Pour mieux se comprendre

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

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

ASSOCIATE MEMBERS

Michael Kert Eisen

Vice-President, Law and Corporate Affairs
Microsoft Canada
1950 Meadowvale Blvd., Mississauga, ON
L5N 8L9
Telephone: (905) 363-8430
Fax: (905) 363-0973
Cell: (416) 434-3737
Email: meisen@microsoft.com



Bio; As Vice-President, Law and Corporate Affairs at Microsoft Canada Co., Michael Eisen is a member of the company's Canadian Leadership Team which is responsible for driving the company's long-term business direction and future growth. He oversees Microsoft Canada's legal needs generally with particular emphasis on government relations, competition policy and intellectual property issues.

Mr. Eisen comes to Microsoft Canada from a prominent Toronto legal firm where he was Secretary and General Counsel to the Canadian Alliance Against Software Theft and Microsoft's lead Canadian outside counsel. Mr. Eisen is a member of the Canadian Bar Association, the Law Societies of Alberta and Upper Canada, and the Licensing Executives Society.

Educated at York University and Osgood Hall Law School he was admitted to the Ontario Bar in 1977 and the Alberta Bar in 1981.

Bessie Pang

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



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

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

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

TECHNICAL ADVISORS

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



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.

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



Department of Justice
Canada

Ministère de la Justice
Canada

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.

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.

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



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



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



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.

Dan Rajsic

Staff Sergeant
Ontario Provincial Police
777 Memorial Avenue
Orillia, ON
L3V 7V3
Telephone: (705) 329-6441
Fax: (705) 329-6369
Email: dan.rajsic@ontario.ca



Bio: Staff Sergeant Dan Rajsic has been a member of the Ontario Provincial Police for 27 years. He is the current Manger of the Electronic Crime Section who's mandate is to provide specialized investigative services facing investigations in which electronic equipment, and/or the Internet are identified as key elements of the investigation.

Staff Sergeant Rajsic spent the first 11 years of his career working in various field positions, such as uniform officer, marine officer, and as a criminal investigator. In 1993 he transferred to the OPP's general headquarters and has provided support to specialized program areas, namely Information Technology Section, Electronic Surveillance Section and the Electronic Crime Section.

Since being engaged in the field of electronic surveillance Staff Sergeant Rajsic has become actively involved in developing strong partnerships with other law enforcement agencies throughout Canada, as well as Industry partners and government working groups. He has provided leadership in the field of electronic surveillance not only within the Electronic Surveillance Section, but as President of the Ontario Technical Investigators Assoc and also by chairing a Federal lawful access committee who have worked aggressively on justifying the need legislative changes in the area of electronic surveillance. Since he transfer to the Electronic Crime Section, he has taken on the responsibility of chair for the National Technological Crime Advisory committee, reporting to the CACP e-Crime committee.

He has tremendous interest in ensuring that law enforcement, nationally, has the appropriate tools to successfully investigate all types of crime in order to support the need for public safety.

Appendix "A"



CACP e-Crime Committee January 21, 2009 – Vancouver, B.C.

Participating:

Tom Pownall (Co-Chair)
Dick Bent
Al Tario, Ottawa,
Mark Chatterbok
France Thibodeau
Bessie Pang
Marc Moreau
Ken MacKay
Martin Charette

RCMP – Ottawa
RCMP - Vancouver
Ottawa Police Service
Saskatoon Police Service
Canadian Police College
Society for the Policing of Cyberspace
RCMP – Ottawa
Edmonton Police Service
Sûreté du Québec

Participating via teleconference:

Kate Lines (Co-Chair)
Dan Rajsic

OPP - Orillia
OPP - Orillia

Regrets:

Ray Archer
Michael Eisen
Randy Robar
Alain Dubuc
Gareth Samson
Alexander Smith
Dan MacRury
Steve Izzett

Canadian Bankers Association – Ontario
Microsoft
RCMP – Charlottetown
Sûreté du Québec
Justice of Canada , Criminal Law Policy
Attorney General, Crown Law Office – (Ont)
Nova Scotia – Public Prosecution Service
Toronto Police Service

1. Opening Remarks

Co-Chair Tom Pownall brought meeting to order and welcomed members able to attend.

2. Membership Issues

Role of Technical Advisors – No new development. Member of the Committee can choose to bring an SME if they see fit.

An effort to recruit an east coast representative continues. The CACP Executive will be contacted to see if they may have someone to recommend in this regard.

3. Review of Previous Minutes

Minutes accepted from last meeting held in Montreal, August 23, 2008.

Recommended by Dick Bent. Seconded by Mark Chatterbok.

Review of correspondence. Message from Peter Cuthbert January 6, 2009. The VP Liaison to our Committee is Jean-Guy Gagnon

4. CIRA (Canadian Internet Registry Authority) - Update

Marc Moreau advised the Committee that CIRA would be evaluating the use of LER (Law Enforcement Request) that came into effect last year on June 10, 2008 and it is expected the RCMP will be called before the CIRA Board to provide an assessment of the use (or the non-use) of the LERs.

CIRA had limited the voluntary disclosures it makes to peace officers by applying rules and procedures it has developed for “Requests for Disclosure of Registrant Information for Law Enforcement”. Peace officers using these LERs needed to be reminded of the limitations and risks involved in seeking voluntary disclosure from CIRA.

The most significant risk to law enforcement is that CIRA will attempt to notify the individual registrant of the dot-ca domain name in question of the disclosure to police between 30 and 60 days after providing the information to police. Therefore, use of LERs will not protect the confidentiality of an ongoing investigation. Furthermore, CIRA has full autonomy in deciding whether or not to accept a peace officer’s LER and voluntarily provide the requested information.

As a result of the discussions at this meeting the consensus from the law enforcement community is that the use of the LER is not worth the risk. However it will be explained

to CIRA that LE had expressed their concern at the onset and those concerns still exist. A longer period for assessment will be requested from CIRA. It is not known what position CIRA will adopt as a result of the assessment. Further information will be provided at a future meeting.

NB: Marc Moreau attended the ICANN meeting in Mexico City, March 1-6, 2009 and moderated a session entitled: Law Enforcement and ccTLDs (country code top level domains) on March 4, 2009. It was interesting to note that some European Union countries were providing the WHOIS information to legitimate LE requests (without any court order). However it seems there are concerns with this practice as the gTLDs are looking to have contracts with LE to provide access approved by a national data protection agency. It is the gTLD view in the EU that LE tends to over-ask as they wanted full access to all of their data. It seems that a solution is being worked out. It will take some time to assess the impact of this approach to determine whether it really meets the needs of all the stakeholders.

5. Review of Draft Best Practices for First Responders to Digital Evidence

Copies of these documents were made available to Committee members prior to this meeting. The document name was amended to: "First Responders Guidelines for Digital Evidence". This document will be posted on the CACP web site in the Members Only area.

Recommended by: Marc Moreau

Seconded by: Dick Bent

France Thibodeau had identified a few minor corrections to the document and these have been addressed. France will be using this document for the DTIC (Digital Technologies for Investigators Course).

As mentioned in the Minutes of the last meeting this document is recognized as a living document it will be submitted to the CACP as a deliverable, with the understanding that amendments will be made when and as required. It is recommended the National Tech Crime Advisory Committee (NTCAC) review this document on a yearly basis.

6. Role of the E-Crime Committee in the Internet Governance

Marc Moreau 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.

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 Internet's 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 two keys to success in this role are the full participation of the international community and collaborative nature of the bottom-up policy development process.

The mission of The Internet Corporation for Assigned Names and Numbers ("ICANN") is to coordinate, at the overall level, the global Internet's systems of unique identifiers, and in particular to ensure the stable and secure operation of the Internet's unique identifier systems. In particular, ICANN:

1. Coordinates the allocation and assignment of the three sets of unique identifiers for the Internet, which are
 - a. Domain names (forming a system referred to as "DNS");
 - b. Internet protocol ("IP") addresses and autonomous system ("AS") numbers; and
 - c. Protocol port and parameter numbers.
2. Coordinates the operation and evolution of the DNS root name server system.
3. Coordinates policy development reasonably and appropriately related to these technical functions.

The RCMP has been attending these meetings that are held in different continents on a rotational basis. The RCMP is 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.

These meetings are open to the public and this committee recommends broader law enforcement participation from the law enforcement community in Canada.

Marc Moreau will be traveling to Washington, DC in February 2009 to attend the first meeting of the ARIN (American Registry for Internet Numbers) and Government Working Group (AGWG). ARIN is one of only 5 Registries worldwide. The efforts of this group will support the overall initiative to gain a voice in the Internet governance. This meeting is a joint initiative being organized by ARIN and the FBI.

7. Review and Approval of Revised CACP E-Crime Committee Strategic Plan

The final document was presented at this meeting. No objections were raised therefore the document is accepted as a final product.

Dick Bent would like to see the Committee take on the task of determining/identifying emergent trends. Discussion regarding the measure of success of the various initiatives ensued. How do we know we have achieved what we have set out to do?

Goal # 1:

To Establish A Leadership Role In The Development of Administrative Policy and Standards for Technology-Based Investigations – Championed by Dick Bent

Dick would like more time to review the initiative and have discussions with NTCAC to determine and identify areas of interest.

Bessie Pang offers the service of the PolCyb and the Simon Fraser University (SFU) International Cyber Crime Research Centre to help the goals and the Strategic Plan.

Dick will meet with them to hold discussions and establish a strategy to move forward.

Goal # 2:

This goal is being held in abeyance at this time as a new person has to be identified to champion this initiative.

Goal # 3:

The Establishment of Proficiency Levels – Championed by Mark Chatterbok

Mark plans to team up with Dick to meet with SFU to better determine the issues in identifying measures of success.

Discussions followed with regards to the national standard for computer forensics that was discussed at the last NTCAC meeting. At that meeting it was agreed that the following courses would be mandatory as the national standard:

- A+ (prerequisite for CMPFOR)

- N+ (prerequisite for NIC)
- Computer Forensics Course (CMPFOR)
- Internet Evidence Analysis Course (IEAC)
- Network Investigators Course (NIC)

** The Cellphone Seizure & Analysis Workshop (CSAW) does not form part of the core courses for a qualified forensic examiner as police services often have personnel that only specialize in cell phones.

Goal #4:

Linkages With Other CACP Committees – Championed by Martin Charette & Ken MacKay

Martin Charette had discussions with various law enforcement agencies. There was also a discussion at the last NTCAC with regards to standardizing the processing of child exploitation images however this is proving to be challenging. The issue is that the Canadian law enforcement community has been unable to come to an agreement as to the number of categories that should be used in the C4P software to categorize the images of child exploitation.

Discussions were also held with regards to data retention. Tom Pownall provided some background information regarding the positions held by various agencies and the resulting challenges that we are still facing.

8. Update of PolCyb

Bessie Pang provided an update of the efforts of CyberPol. The next international conference will be held in Budapest in September 2009. A North American region conference is also planned for mid-June. Looking to invite an ICANN representative to attend.

There is software available (artificial intelligence) as a data-mining tool developed at University of Arizona for law enforcement called the AI Lab Dark Web project. It is available to law enforcement (at no cost) as the University is open to hear from LE regarding its use. Here is a description from its web site (<http://ai.arizona.edu/research/terror/index.htm>):

The AI Lab Dark Web project is a long-term scientific research program that aims to study and understand the international terrorism (Jihadist) phenomena via a computational, data-centric approach.

We have developed various multilingual data mining, text mining, and web mining techniques to perform link analysis, content analysis, web metrics (technical sophistication) analysis, sentiment analysis, authorship analysis, and video analysis in our research.

The approaches and methods developed in this project contribute to advancing the field of Intelligence and Security Informatics (ISI). Such advances will help related stakeholders to perform terrorism research and facilitate international security and peace.

On another note Bessie advises that Sierra Systems is setting up a PolCyb portal secure area available for members only.

9. National Tech Crime Advisory Committee (NTCAC) - Update

Dan provided an update of the last meeting held in Niagara Falls, October 29/30, 2008. Minutes of that meeting were distributed to this Committee.

10. Canadian Police College - Update

France Thibodeau provided a briefing about the Digital Evidence Foundation that speak to certification and re-qualification issue. She has been identified as the Canadian representative and will seek more information and report back to this Committee and the NTCAC.

France also gave an update of the CPC for 2009 such as:

- Live state analysis
- FTK and Vista on the CMPFOR course
- NIT – more scenario based
- CSAW in Calgary
- Now 4 CMPFOR courses for 2009 (instead of only 2 in 2008)
- The CPC is also looking into the possibility of developing more on-line courses.

11. Outstanding Resolutions – Next Steps

Ken MacKay will follow-up with the Law Amendments Committee (LAC) to assess where we stand with regards to the 2 outstanding Resolutions #08-2006 and #07-2007.

12. Emerging Issues

- 1-) Use of Civilian employees vs police officers for computer forensics
- 2-) ISO Standard – for information purposes only at this time
- 3-) NPS (National Police Services) proposal - Tom Pownall spoke about the possibility of looking at this model that could potentially better meet the needs of this specialized field. Dick Bent expressed an interest to look at something that already exists in BC that speaks to this possibility. Ken MacKay would agree so long as adequate funding is in place for this purpose. Al Tario advises there is minimum level of service that just came out in Ontario. There is support from the group to look into this further (include regional). This merits more attention.
- 4-) CERT Virtual Training. Being assessed and evaluated by the RCMP/CPC. More information to follow.

Next meeting will take place at Canadian Bankers Association, Merchant's Boardroom (199 Bay street, 30th Floor, Toronto, also known as Commerce Court West - corner of Bay St and King St) on June 4, 2009 starting at 9am.

Appendix "B"



CACP E-crime meeting June 4, 2009 Toronto, Ontario

Participating:

Tom Pownall (Co-Chair)
Kate Lines (Co-Chair)
Al Tario, Ottawa,
Mark Chatterbok
Ken MacKay
Martin Charette
Tom Fitzgerald
Ray Archer
Marc Moreau
Dan Rajsic

RCMP – Ottawa
OPP - Orillia
Ottawa Police Service
Saskatoon Police Service
Edmonton Police Service
Sûreté du Québec
Toronto Police Service
Canadian Bankers Association – Ontario
RCMP – Ottawa
OPP - Orillia

Participating via teleconference:

Bessie Pang Society for the Policing of Cyberspace

Regrets:

France Thibodeau
Michael Eisen
Randy Robar
Gareth Samson
Alexander Smith
Dan MacRury
Service

Canadian Police College
Microsoft
RCMP – Charlottetown
Justice of Canada , Criminal Law Policy
Attorney General, Crown Law Office – (Ont)
Nova Scotia – Public Prosecution

Guests:

Peter Cuthbert – Executive Director, CACP
Det. Maureen Bryden – Ottawa Police Service

1. Opening Remarks

Co-Chair Tom Pownall brought meeting to order and welcomed members able to attend.

2. Membership Issues

Given the fact the C/Supt Dick Bent is retiring from the RCMP this Committee will be looking for some replacement. The following names were suggested:

A/Comm'r Peter German, RCMP, "E" Div
Frank Beasley – Halifax PS

3. Review of Previous Minutes and Correspondence

Minutes. Minutes accepted from last meeting held in Vancouver, January 21, 2009. Recommended by Ray Archer and seconded by Martin Charette

Review of correspondence. Kate received a letter from the Law Amendments Committee to attend a meeting on April 24, 2009 with regards to the Sex Offender Registry. She presented at the Parliamentary Review Committee on that date.

Peter mentioned that the National Child Exploitation Coordination Centre (NCECC) conference was being held in Montreal this week and it was proving to be a great success. Approx 60 lawyers were in attendance and this was proving to be enhancing the level of discussions with law enforcement in these types of investigations.

4. Provincial Strategy on Child Pornography – Det Maureen Bryden, Ottawa PS

Det Bryden gave an excellent presentation that covered the following points:

- Who is HTC-ICE Unit
- Mandate
- Roles and Responsibilities
- Provincial Strategy – 18 PS across Ontario which resulted in the following:
 - ✓ 38 Criminal Code search warrants executed simultaneously throughout province of Ontario

- ✓ 35 Persons arrested
- ✓ Over 100 Criminal charges laid

- National Strategy (Operation SALVO)- March 2009
 - ✓ 40 police agencies
 - ✓ 60 search warrants executed
 - ✓ 103 criminal charges laid

- Lessons learned

5. CACP Update – Peter Cuthbert, Executive Director, CACP

Peter Cuthbert shared the following items from his CACP Board of Director meeting held March 7, 2009 in Vancouver:

- 103rd Annual Conference - 2008 Montreal

- CACP Annual Conference - 2009 Charlottetown, PEI - encourage members to register and seek accommodations.

- Professional Development Program on website

- 106 Annual Conference - Edmonton AB.

- National Framework for Progressive Policing in Canada - Priority #1 for CACP, Committee working with Canadian Association For Police Boards / Canadian Police Association/ Federation of Canadian Municipalities

- Encouraged E-Crime Committee to work with Ruth Montgomery to assist her with the Resolutions Status Report

- Reviewed Conducted Energy Weapons Policy

- Discussed CACP events (May to December, 2009)

- Discussed 18th Committee of the CACP - International Committee

- Reviewed Nomination Committee Guidelines

- Discussed the CACP's Strategic Planning Priorities

- Provided a status report on the CACP Finances
- Advised the Committee of the potential to purchase a new office complex
- We discussed the Safer & Healthier Canada Fund - \$5000. grant to E-Crime
- Supt. Tom Pownall discussed his participation in the Institute for Strategic International Studies (ISIS) Program

6. National Tech Crime Advisory Committee – NTCAC Update – S/Sgt Dan Rajsic, OPP

As Chair of the NTACA, S/Sgt Dan Rajsic provided an update of the last NTCAC meeting that was held in Ottawa April 29-30, 2009. The following information will also serve as a Summary of the NTCAC in preparation of the CACP Annual Meeting.

CIRA

Since June 10, 2008, CIRA no longer made registrant information for individual registrants of dot-ca web sites publicly available through its on-line WHOIS look-up directory. WHOIS is an electronic look-up service available from the cira.ca website.

CIRA indicated that it will accept requests from peace officers to voluntarily provide such information in very limited circumstances through the use of LER (Law Enforcement Request). In all other cases, CIRA says peace officers requiring this information for investigative purposes can obtain it by presenting CIRA with a court-issued production order. The largest concern was that CIRA would eventually notify the registrant that law enforcement had made an inquiry - very problematic to the police.

CIRA were to review this policy after one year so they are now contacting some police agencies to conduct surveys and report back to government on their findings.

As of July 13, 2009, no members from the NTCAC committee have been contacted but it is anticipated contact will be completed by the end of the summer.

Understudy Guide

The NTCAC has successfully developed a recommended Guide for Understudy - Technical Investigator. This was completed with the assistance of the CPC as it outlines the required CPC courses that should be completed by anyone in an

Understudy program. The guide was brought forward at the last CACP e-Crime committee meeting in Toronto seeking approval.

Department of Justice (DOJ) - Criminal Code revisions

The NTCAC have commenced to strengthen their working relationship with the DOJ's Policy Advisory group who are tasked with updating legislation. This working group attended the NTCAC's April 2009 meeting to discuss the proposed changes to Part XV, later incorporated in bill C-46, Investigative Powers for the 21st Century Act.

The DOJ Policy Advisory group have asked to attend the next NTCAC meeting to discuss future changes to the Criminal Code in regards to computer crimes or offences associated to digital technologies. It is imperative that these relationships remain positive as law enforcement can truly inform the Policy Advisors what will and will not work, operationally, when it comes to new legislation.

Use of Encryption

This is a growing concern when investigations involve seized encrypted data. The federal government, specifically the DOJ, recently completed a survey that was intended to determine the amount of encrypted data seized for examination by law enforcement. It was noted that although the current percentages between encrypted and clear data is very low, it is on the incline and will become extremely problematic.

A new survey was to be distributed so we can have a closer look at where law enforcement is continuously encountering encryption - such as mobile devices compared to computer hard drives.

NOTE: The CACP e-Crime committee filed resolution 2007-06, Lawful Access to Encrypted Electronic Media Commentary, which is still pending.

Future Meeting Discussions:

- Use of civilians to complete forensic analysis - there is differences in opinions between technical crime sections on this topic.
- Disclosure of digital evidence in cases involving child pornography.

- Out sourcing of work for forensic analysis - all technical crime section's workloads are extreme but there are many concerns with using out sourcing as a viable option.
- Other agenda topics that will directly support the strategic plan of the CACP e-Crime committee.

7. Internet Governance Update – Internet Corporation of Assigned Names & Numbers (ICANN) and Canadian Internet Registration Authority (CIRA) – Update by Marc Moreau and Martin Charette

Marc Moreau provided an update of the ICANN meeting that was held in Mexico City, March 1-6, 2009. Martin Charette also attended this meeting. Marc was on a Panel as well as a Moderator at one of the law enforcement break-out sessions. Attending these ICANN meetings affords law enforcement worldwide an opportunity to gain traction within the internet community to voice issues/concerns faced by LE. There were other members of the Strategic Alliance Group (ie: USA, UK, Australia, New Zealand and Canada) also in attendance (ie: FBI, SOCA - Serious Organized Crime Agency, UK,). Marc Moreau also provided an update on CIRA. On June 10, 2008, CIRA had introduced a policy that restricted the WHOIS information with regards to an individual registrant on the dot CA domain. On behalf of the Canadian law enforcement community the RCMP was able to negotiate a compromise with CIRA whereby Law Enforcement Requests could be used in certain investigations (ie: National security, child exploitation) and CIRA would provide the subscriber information (of an individual) without a warrant. However, CIRA remained firm on their intent to advise the subscriber within the following 60-90 days. This procedure/compromise has now been in effect for close to 1 year and we expect to hear from CIRA to assess this procedure. At the time of this meeting we had heard that apparently no law enforcement requests were received by CIRA however it is somewhat obvious why a LEA would hesitate to make use of same (due to the disclosure to the subscriber by CIRA)

From a law enforcement perspective we intended to re-iterate to CIRA that the WHOIS database should not be restricted as it is a widely accessible database in most other countries. At the very least we would have argued that the assessment period be extended for a longer period to see what may develop.

However, on June 18, 2009 the Minister of Public Safety successfully introduced Bill C-47 before the current government. It is entitled the Technical Assistance for Law Enforcement in the 21st Century Act. The purpose of this Act, Section 3 is:

The purpose of this Act is to ensure that telecommunications service providers have the capability to enable national security and law enforcement agencies to exercise their authority to intercept communications and to require telecommunications service providers to provide subscriber information, without

unreasonably impairing the privacy of individuals, the provision of telecommunications services to Canadians or the competitiveness of the Canadian telecommunication industry.

* S/Sgt Marc Moreau has been identified to be interviewed by a consulting firm that has been hired by CIRA for the evaluation of their privacy policy. This interview will be conducted on June 23, 2009
More information to follow.

8. CACP E-Crime Committee Strategic Plan – Mark Chatterbok/Bessie Pang

On March 4, 2009, Bessie, Dick and Mark met with Dr. Bill Glackman, director of the Criminology Research Centre at Simon Fraser University. The purpose of the meeting was to determine if the International Cybercrime Research Centre would be able to assist us in establishing a measurement/evaluation model for the eCrime strategic plan, or assist us with other research topics that would be valuable to eCrime investigators.

As a result of this meeting, we identified 3 potential research projects that the Research Centre may be able to assist us with.

1. Conduct an environmental scan regarding eCrime trends and the types of investigations that are being conducted in other countries
2. Identify current impediments to eCrime investigations (eg. training, prosecutions, computer forensics)
3. Categorize programs and information available from other countries and collate the information and make available on the POLCYB website

The meeting ended with a recommendation to update the eCrime Committee regarding the possible research topics and to await direction from the eCrime Committee prior to moving ahead with this initiative.

9. PolCyb Activities in 2009

POLCYB Workshop, Vancouver, June 8th, 2009:

http://www.polcyb.org/workshop_2009/workshop_2009.html; Event sponsored by Sierra Systems Group Inc. Preliminary

Programme:http://www.polcyb.org/workshop_2009/programme.html Option for WebEx

participation available. If any E-Crime members wish to join the Workshop via WebEx, please register by June 7th.

9th Annual Policing Cyberspace Summit 2009, October 5th - 8th, 2009, Budapest, Hungary:http://www.polcyb.org/summit_2009/summit_2009.html - Announcement attached. The Summit is co-hosted by the International Law Enforcement Academy (ILEA) Budapest, Hungary, and organized in collaboration with the Council of Europe (COE). The Summit Theme is: "Implications of Emerging Technologies Upon Cybercrime Prevention and Response". Please also note the info. on the Annual POLCYB International Law Enforcement Cybercrime Award 2009 (ILECA) in the attached.

Nigel Jones contacted Bessie to advise on the 2CENTRE Proposal - www.2centre.eu I wish to bring their proposal to E-Crime Committee's attention for information.

Update on POLCYB Portal - Sierra Systems is in the process of assisting POLCYB to provide an interim phase for our international members to benefit from the new "Resources" feature, while Sierra works on developing Content Management System portion of the POLCYB Trusted Community Portal. The POLCYB Portal was discussed in the previous E-Crime Meeting. The new POLCYB website should be launched this summer. We're hoping launch the Portal portion by the time the POLCYB Summit is held in October 2009. Upon completion of the POLCYB Portal, POLCYB will contact administrators of related portals from other organizations to join, e.g. the Global Prosecutors E-Crime Network (GPEN) <http://www.gpen.info/>.

10. Strategic Alliance Group (SAG) – Update by Tom Pownall

Background Information:

In September 2006, police services from Australia, Canada, New Zealand, the United Kingdom, and the United States met at FBI Headquarters and formed the **Strategic Alliance Cyber Crime Working Group**

Collectively developed a comprehensive overview of the transnational cyber threat—including current and emerging trends, vulnerabilities, and strategic initiatives for the working group to pursue (note: the report is available only to law enforcement)

- There is an increasing requirement for law enforcement to engage the Internet community from a global perspective.

- This is a priority activity of the FBI, SOCA and AFP and there is an expectation from the international law enforcement community that Canada will actively contribute to this endeavour.
- Given the potential future impact on operational law enforcement activities and criminal investigations, it is imperative that law enforcement pro-actively engage key partners in matters related to Internet governance.

At the last meeting the SAG discussed the operational coordination on transnational on-line organized crime. Tom will continue to update the group regarding the progress of this group.

As well the SAG produced 2 Cyber Crime Information Bulletins that were shared with the members of this Committee for this meeting.

11. Next Steps

Next meeting will be in Charlottetown for the CACP Annual meeting in August. The consensus of the group indicated that only a few people were intending/available to attend the E-Crime meeting. As a result it was decided that a teleconference will be scheduled for the Friday afternoon, 2009-08-07, at 14:00hrs (PEI time) for anyone available to join. The Annual E-Crime Report will be tabled at this meeting. The Fall meeting tentatively set for November 19, 2009 in Orillia, Ontario (OPP).

12. Emerging Issues/Threats

- 1-) Conficker worm
- 2-) Man in the browser (MitB)

Appendix "C"

List of members for the National Tech Crime Advisory Committee

NAME	AGENCY
Dan Rajsic	Ontario Provincial Police
Shawn Nash	Ontario Provincial Police
Marc Moreau	RCMP TPOF
Kevin Mallay	RCMP - East Coast
John Revitt	Vancouver PD
Kevin McQuiggin	Vancouver PD
LeeAnn Papizewski	Toronto Police Service
Cindy Childs	Toronto Police Service
Martin Charette	Surete du Quebec
Il Kim	Surete du Quebec
Palamattam	Edmonton PS
Francesco Secondi	Montreal PS
Jeff Mitchell	Peel Regional PS
Ryan Duquette	Peel Regional PS
James Stewart-Haass	Durham Regional PS
Monique Perras	Ottawa PS
Bill Hasenpflug	Winnipeg PS
Dick Nyenhuis	Calgary PS
Craig Coughlin	Calgary PS
Robert Armstrong	York Regional PS