Resolutions adopted at the 110th Annual Conference

August, 2015
Quebec City, Quebec

CANADIAN ASSOCIATION OF CHIEFS OF POLICE
Safety and security for all Canadians through innovative police leadership

Unit 100 – 300 Terry Fox Drive, Kanata Ontario K2K 0E3
p: 613-595-1101 f: 613-383-0372
e: cacp@cacp.ca w: www.cacp.ca

Table of Contents

Resolution #01 - 2015

DEVELOPMENT OF A NATIONAL FRAMEWORK ON PROACTIVE COMMUNITY-POLICING RESPONSES TO DOMESTIC AND INTIMATE PARTNER VIOLENCE

Submitted by the Crime Prevention, Community Safety and Wellbeing Committee

WHEREAS the Crime Prevention, Community Safety and Wellbeing Committee (CPCSW) planned initiatives for 2014/2015 which include exploring "opportunities to coordinate crime prevention and domestic and intimate partner violence initiatives", and recognized that addressing police proaction and response to domestic and intimate partner violence (D/IPV) requires multi-sectoral collaboration due to the complex social and criminal elements that are rooted in homes and relationships, and;

WHEREAS D/IVP is a complex social and criminal issue with indisputable human and financial costs, (estimated at $7.4 billion per year in Canada), and accounts for approximately one quarter of all police-reported violent crime and the victimization of nearly 95,000 citizens annually, and;

WHEREAS D/IPV can be more effectively and efficiently addressed through the fundamental principles of contemporary community policing; an approach that emphasizes problem identification, root cause analysis, education, prevention, intervention, response, support, evaluation and collaboration among police and non-police sectors, and;

WHEREAS the CPCSW Committee is comprised of police leaders and strategic community leaders from government and non-government organizations who possess expertise in the areas of DIPV and gender-based analysis, and has worked in partnership with the *Canadian Observatory on Justice System Response to Intimate Partner Violence*, and in the creation of a 2014 "Think Tank" on D/IPV that brought together 35 subject matter experts including police, academics and practitioners to share best practices from their respective regions, and;

WHEREAS "D/IPV Think Tank" participants agreed that a unified police model for D/IVP in Canada is critical to create shared understanding, consistent terminology and common application of the law and police practice, and that this may be achieved through a National Framework, and;

WHEREAS the "D/IPV Think Tank" led to the creation of an expert working group, designed to establish a national community of practice on police proaction, intervention and response, and;

WHEREAS the CPCSW Committee endorses the development of a National Framework on Proactive Community-Policing Responses to Domestic and Intimate Partner Violence and has approved the creation of a subcommittee to explore the issue of D/IPV as it relates to creating safer communities through police and partnership action, and the establishment of a community of practice, and;

WHEREAS the CACP has previously endorsed national standards as a means of promoting common principles.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police recognizes and endorses the development of a National Framework on Proactive Community-Policing Responses to Domestic and Intimate Partner Violence, to be led by the Crime Prevention Community Safety and Wellbeing subcommittee, in partnership with the Canadian Observatory on the Justice System's Response to Intimate Partner Violence.

Resolution #01 - 2015

DEVELOPMENT OF A NATIONAL FRAMEWORK ON PROACTIVE COMMUNITY-POLICING RESPONSES TO DOMESTIC AND INTIMATE PARTNER VIOLENCE

Background

D/IPV is a complex social and criminal issue that carries a high, indisputable human and financial cost in our society, with a total economic impact in Canada estimated at $7.4 billion per year. (Zhang, et al. 2012). In 2011, family violence accounted for 26% of all police-reported violent (Statistics Canada, 2013), and about half (49%) of the nearly 95,000 victims of family violence were in a current or previous spousal relationship.

Research continues to show that police intervention and response to D/IPV can be more effective and efficient through the use of the principles of contemporary community policing, as evidenced by initiatives like Crime Prevention Through Social Development, the Hub and Core and Prolific Offender models.

In 2014, the CACP approved a name change to its Crime Prevention Committee, in order to better reflect the mandate of CACP and the Committee itself. The Committee is now known as the CACP Crime Prevention, Community Safety and Wellbeing Committee (CPCSWC).

At the 2014 CACP Annual General Meeting, the CPCSWC also introduced Resolution 2014-02, to change the conversation from the "Economics of Policing" to the "Economics of Community Safety and Wellbeing," in its ongoing work to raise awareness that complex costs of public safety are related not only to police, but to a variety of non-police sectors working to encourage prosocial behaviour, prevent crime and social disorder, and address the needs of those who come into contact with the criminal justice system (CACP Resolution #02 - 2014).

In May 2014, through a partnership between New Brunswick Police Forces (Fredericton, Saint John and RCMP "J" Division) and the Canadian Observatory on the Justice System Response to Intimate Partner Violence, a "National Think Tank" was held entitled "Community Police Response to Intimate Partner Violence (IPV): Sharing Best Practices." This meeting, sponsored by the Canadian Observatory and the Muriel McQueen Fergusson Centre for Family Violence, brought together 35 ranking police officers and academics, to discuss various best practices developed and implemented by police forces across Canada, while also creating a "knowledge building community." Think Tank participants agreed that a unified police response to D/IVP in Canada, including consistent terminology and common application of the law, is critical to enhancing the national response to this issue.

The Canadian Observatory on the Justice System's Response to Intimate Partner Violence is an international network of researchers, practitioners and policy-makers from across many disciplines focusing on identifying policies and strategies to resolve intimate partner violence and exploring how the justice system functions across the country and abroad. It is housed at the University of New Brunswick, under the leadership of Dr. Carmen Gill in the Department of Sociology.

Resolution #02 - 2015

SEIZURE OF CELLULAR TELEPHONE SERVICES WHEN USED IN DRUG TRAFFICKING

Submitted by the British Columbia Chiefs of Police (BCACP)

WHEREAS a significant component of drug trafficking at the street level involves communication between the customer (drug user) and the seller (drug trafficker) via cellular telephone or other mobile devices (referred to “dial-a-dope” operations), and;

WHEREAS through “dial-a-dope” operations, drug traffickers are able to make it widely known within the drug-trafficking community that certain telephone numbers are a means to quickly facilitate drug trafficking, and;

WHEREAS there are currently no lawful means by which law enforcement can "seize" or take possession of a non-tangible item (such as a cellular phone line/number), or to otherwise deactivate a cellular phone line/number pursuant to the Criminal Code or Controlled Drug and Substances Act, either during investigation or post-arrest, and;

WHEREAS without the ability to seize or terminate the cellular phone line/number, the specific number continues to be available to facilitate the illicit trafficking of drugs, and;

WHEREAS despite the significant efforts by law enforcement to disrupt drug trafficking operations, “dial-a-dope” traffickers remain a significant problem for Canadian communities. In particular, “dial-a-dope” operations are often associated with violence against persons, and;

WHEREAS in 2015, the British Columbia Association of Chiefs of Police passed a resolution requesting the Canadian Association of Chiefs of Police Law Amendments Committee identify a means for law enforcement to seize or otherwise nullify (deactivate) the phone lines/numbers associated with “Dial-a-Dope” operations, in order to disrupt that criminal activity, and;

WHEREAS through study it has been determined that this matter can only be addressed through amendments to legislation or through new legislation.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police urges the Government of Canada to identify a legislative means for law enforcement to seize or otherwise nullify phone lines/numbers used by drug traffickers in “Dial-a-Dope” operations.

Resolution #02 - 2015

SEIZURE OF CELLULAR TELEPHONE SERVICES WHEN USED IN DRUG TRAFFICKING

Background

A significant component of drug trafficking at the street level involves communication between the customer (drug user) and the seller (drug trafficker) via cellular telephone or other mobile devices (referred to “dial-a-dope” operations).

A "dial-a-dope" transaction typically begins with the procurement of a telephone number by the drug trafficker or part of his/her criminal network. This telephone number is then advertised through a variety of means including business cards and word of mouth, through the existing drug culture/network, with the intent of attracting potential customers. A potential customer then calls the number, provides a predetermined code or other information to verify that they are a customer (as opposed to a police officer), and then arranges for a drug purchase. The drug trafficker then meets the customer at the specified location and the drug transaction occurs. Once a person has been established as a “real” customer, some drug lines also use text messaging functions to arrange future transactions, leveraging the voice and data capabilities of the service providers. The use of cellular communications, coupled with vehicle delivery, allows for these drug transactions to be completed very quickly with limited potential for apprehension by law enforcement.

“Dial-a-dope” operations can be very lucrative for the trafficker. Once a telephone number or "drug line" has been established, it can operate non-stop at all hours of the day and distribute drugs to a broad base of customers across a significant geographical area. As a result, once established, each drug line has an inherent value within the drug trafficking realm and can be bought, traded or taken over by rival drug trafficking networks. Simply stated, the specific phone line/number is a significant asset to the drug trafficker.

EFFECTIVENESS OF CURRENT LAW ENFORCEMENT STRATEGIES:

Law enforcement has had limited success addressing these drug lines. Typically, intelligence is obtained that a specific phone number is a drug line. Background investigation into that phone number occurs, including the police obtaining the subscriber information. The investigators look closely at the information to address case law decisions relating to issues such as entrapment or random virtue testing. If appropriate grounds still exist, an undercover operator posing as a drug user/purchaser calls the drug line. If successful in providing the appropriate code phrase or other information, the drug transaction occurs and those persons involved in the sale itself are arrested and charged. However, the specific phone line/number still exists and most often continues to be used to facilitate the illicit drug trafficking operation.

Where possible, the vehicles and devices themselves used to commit the offence are seized as Offence Related Property. However, as stated above, the telephone line/number itself remains active. There are presently no lawful means by which law enforcement can "seize" or take possession of the (non-tangible) phone line/number.

The drug trafficking network continues to exist (usually with a new code phrase), another vehicle is obtained, and a new cellular telephone is acquired and connected to the existing phone number. The point-of-contact between the purchaser and trafficker continues virtually unimpeded. In addition, the longer a drug line exists, the better known it becomes, resulting in more "customer" use and greater risk to public safety.

EFFORTS TO SEVER COMMUNICATION NETWORKS OF DRUG TRAFFICKERS:

The Surrey RCMP Detachment has examined a variety of potential solutions to disrupt the continued use of a telephone number or service by drug traffickers, including the following:

- **Asking service providers to suspend service** where the phone line/number has been used to facilitate criminal activity. This has not been successful, as service providers are reluctant to suspend service to a paying customer, often citing the potential for civil liability and other associated costs. Some service providers may be willing to engage in further discussion if the law enforcement agency accepts any civil liability and associated litigation costs of the service provider, which is not viable. In short, reliance on the corporate conscience of the phone line/number service providers is neither a practical nor effective strategy.
- **Asking the regulatory agencies to suspend service**. Although the CRTC and specifically the Canadian Wireless Telecommunication Association (CWTA) engage with service providers with regard to the telecommunication industry in Canada, their framework is largely regulatory in nature, making their ability to impact the broader criminal issue of drug trafficking limited. Though these regulatory agencies have participated in recent law enforcement initiatives such as the online listing of stolen cellular phone serial numbers in an effort to combat cellular phone theft, they have expressed reservations in directing service providers to suspend service solely at the request of law enforcement. It would appear that their engagement in law enforcement issues is largely in response to potential negative media pressure exerted by outside interest groups.
- **Denial of Service Technology.** Recently, significant effort has been expended to explore the use of automated telephone dialing technologies, similar to those used by telemarketers, to interrupt "dial-a-dope" communications networks. This can be accomplished through the use of auto-dialing computers that call the drug traffickers phone number with sufficient frequency to render the phone number unusable. However, this technique is essentially a "denial of service" attack and contravenes Section 430 of the *Criminal Code*. Although Section 25.1 of the *Criminal Code* provides some potential for the use of a Law Enforcement exemption for this

technique, current legal opinions do not support the use of s. 25.1 to justify such a technique, as such a use is not believed to be consistent with the legislative intent behind s. 25.1.

- **Seeking civil forfeiture of the telecommunication service**. Currently there is no ability for a service such as a telecommunication service (phone line/number) to be seized. For this reason, civil forfeiture is not a viable means of resolving this problem.

LEGISLATIVE CHANGE PROPOSED AND IMPACTS ON DRUG TRAFFICKING:

Drug traffickers have demonstrated the ability to continually adapt to law enforcement efforts to disrupt their criminal activity. They regularly identify gaps in current legislation that work in favour of their criminal operations. The Offence Related Property (ORP) provisions in the *Criminal Code* and *Controlled Drugs and Substances Act* (CDSA) have proven to be highly effective at immediately impacting an offender's ability to conduct illicit activities. The seizure of vehicles, cash, dwelling houses, and telephone hardware has an immediate impact on criminal operations. This is due to the fact that the ORP provisions allow for the immediate seizure of the very tools that criminals use to facilitate their activities. However, the ORP provisions of the CCC and CDSA are directly linked to the definition of "property" within those acts, which does not include non-tangible items such as communications services or a specific phone line/number.

It may be possible to draft amendments that would either expand the definition of "property" or create specific provisions within the ORP framework that would allow for the "seizure" or some other form of deactivation of phone lines/numbers used for "dial-a-dope" operations. However, it is likely that attempts to legislate in this area would be very complex as essentially, the legal underpinnings of both the ORP and restraint provisions of the CC and CDSA relate to actual things that can be seized.

Accordingly, it is the recommendation of the Canadian Association of Chiefs of Police that legislation be enacted for law enforcement to seize or otherwise nullify a phone number that has been or being used in a "dial-a-dope" operation.

Resolution #03 - 2015

REASONABLE LAW TO ADDRESS IMPACT OF SUPREME COURT OF CANADA DECISION *R. v SPENCER, 2014, SCC 43*

Submitted by the E-Crimes Committee

WHEREAS law enforcement requires real-time, or near real-time access to basic subscriber (customer name and address) information (BSI) as it relates to telecommunications' customers for investigative reasons, and;

WHEREAS the Supreme Court of Canada, in their majority decision in *R. v Spencer, 2014 SCC 43*, did state that:

- a reasonable expectation of privacy exists in the identity of an internet subscriber where there is an ability to link that identity to specific online activity;
- the identity of a person linked to their use of the Internet must be recognized as giving rise to a privacy interest beyond that inherent in the person's name address and telephone number found in the subscriber information;
- absent an exigent circumstance, or authority from a reasonable law, such as authority from a judicial warrant or order, police do not have the power to conduct a search for basic subscriber information (BSI) when there exists a reasonable expectation of privacy in that information, and;

WHEREAS since the Spencer decision, the telecommunications companies refuse to provide any basic subscriber information (BSI) in the absence of an exigent circumstance, or a judicial warrant or order, even where there exists no reasonable expectation of privacy, and;

WHEREAS there exists no lawful authority designed specifically to require the provision of basic subscriber information, and the problems posed by this gap in the law are particularly acute where there exists no reasonable expectation of privacy in that information.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police supports the creation of a reasonable law designed to specifically provide law enforcement the ability to obtain, in real-time or near real-time, basic subscriber information (BSI) from telecommunications providers.

Resolution #03 - 2015

REASONABLE LAW TO ADDRESS IMPACT OF SUPREME COURT OF CANADA DECISION *R. v SPENCER, 2014, SCC 43*

Background

In June 2014, the Supreme Court of Canada issued a decision in the case of *R v. Spencer* - identifying that subscriber information that allows for the linking of the identity of a person with specific online activity in the context of a criminal investigation engages a high level of informational privacy. However, telecommunications and other service providers (e.g. financial institutions, rental companies) have interpreted the court's findings more broadly, and now demand judicial authorization (based on a reasonable grounds to believe threshold) for nearly all types of government requests for basic identifying information, extending beyond instances involving a person's substantive Internet activity.

The impact of the Spencer ruling and the broader response by telecommunications and other service providers is having a significant impact on law enforcement and criminal investigations. Basic identifying information is often required at the onset of an investigation where technology plays a role, but the judicial threshold required to obtain warrants and general production orders to access basic identifying information is difficult, and often impossible, to satisfy when an investigation is in its early stages.

Moreover, the impact of the Spencer ruling has caused substantial resource and workload challenges for law enforcement. For example, prior to the Spencer ruling, law enforcement agencies would generally complete a voluntary request to telecommunications service providers for basic identifying information in under an hour, and receive a response from service providers within the same day. Following the Spencer ruling, accessing the same information now often requires ten to twenty times the amount of administrative work and documentation, days of preparation to seek judicial authorization, and responses from service providers can take upwards of one month - sometimes exceeding a service provider's data retention schedule for the same information (meaning the information is no longer available).

Criminal investigations impacted by the Spencer ruling are now often delayed and in some cases, not pursued, due to judicial authorization or resource challenges. This impact applies to a range of investigative work, such as cases involving suspected online child sexual exploitation and abuse, fraud and other financially-motivated crimes, organized crime, requests for international law enforcement assistance, and national security matters involving suspected extremism and other threats to Canada - all of which may require basic identifying information from a telecommunications or other service provider to identify potential evidence for criminal investigations and prosecutions.

Transparency Guidelines

Transparency Reporting Guidelines were prepared by Industry Canada, in consultation with RCMP and other relevant Government of Canada partners, to help private organizations be open with their customers, regarding the management and sharing of their personal information with

government, while respecting the work of law enforcement, national security agencies, and regulatory authorities. Specifically, the Guidelines cover categories of disclosures for reporting purposes and limitations to consider when reporting statistics. Of note, the Guidelines specify that there should be a six month delay in reporting timeframe to ensure that most active investigations have no possibility of being compromised. On June 30, 2015, the Transparency Reporting Guidelines were published on Industry Canada's website: http://www.ic.gc.ca/eic/site/smt-gst.nsf/eng/sf11057.html

Coordinating Committee of Senior Officials

Recently, a discussion paper, led by Justice, was presented to the Federal, Provincial and Territorial Coordinating Committee of Senior Officials, Cybercrime Working Group. The paper focuses on the impact of Spencer and legislative reform considerations.

- Option 1: Create an administrative (non-judicial) scheme for access to Basic Subscriber Information (BSI).
- Option 2: Create a new judicial order (production order) for basic subscriber information and/or add BSI to existing production orders.
- Option 3: Create a specific production order for some types of basic subscriber information with a greater expectation of privacy, and create a specific administrative (non-judicial) authority for access to other types of basic subscriber information.

Recent Case Law

- Since the Supreme Court of Canada released its decision in *R. v. Spencer* in June 2014, case law has started to emerge that applies the analysis in Spencer to other cases involving police requests for BSI.
- The majority of relevant cases thus far are from Ontario and involve requests for BSI associated to a phone number. The cases have generally found that the privacy interests in BSI associated to a phone number are not the same as the privacy interests in BSI linked to an IP address, and distinguish Spencer on that basis. As such, the Ontario decisions have upheld warrantless requests for BSI associated to phone numbers as they found in the circumstances of each case that there was no expectation of privacy in such information. See: *R. v. Morrison* (unreported, Ontario Court of Justice, Reasons released on December 17, 2014); *R. v. Khan* (2014 ONSC 5664); *R. v. Latiff* (2015 ONSC 1580); *R. v. Nurse and Plummer* (2014 ONSC 6004).
- The issue of whether there is a reasonable expectation of privacy in BSI associated to a phone number has also emerged in the context of transmission data recorders warrants (TDRW). These warrants provide judicial authorization to record incoming and outgoing dialed phone numbers. In Ontario, police/Crowns have argued before the Superior Court of Justice that an assistance order is the proper authorization to obtain in conjunction with a TDRW to compel a service provider to provide the BSI associated with the dialed numbers. However, Telus has argued that due to the privacy interests in BSI, as found in Spencer, a general warrant is the proper authorization. Nordheimer J. agreed with the police/Crown and held that Spencer was a decision dealing with the Internet and it did not find that there is always a reasonable expectation of privacy in BSI, but rather it will depend on the circumstances of each case. This is a very recent decision (June 19, 2015), and it will be interesting to see if other jurisdictions follow this reasoning. See *H.M.Q. v. TELUS Communications Company*, 2015 ONSC 3964.

Resolution #04 – 2015

AMENDMENTS TO SECTION 183 of the CRIMINAL CODE

Submitted by the Law Amendments Committee

WHEREAS Canadian Police Leaders are concerned with a number of criminal offences for which the interception of private communications is not a legal investigative option, and;

WHEREAS there are instances when police need to gather additional evidence after traditional investigative means have failed to resolve an investigation, and the use of a judicial authorization to intercept private communication may assist in holding those responsible for causing serious injury or death to someone accountable, and;

WHEREAS there is an ongoing need to increase the number of criminal offences that are included in section 183 of the Criminal Code as offences for which the interception of private communications is lawful through judicial authorization, and;

WHEREAS the Canadian Association of Chiefs of Police, as the national voice of Canadian police leadership, is committed to raising issues where the Criminal Code should be amended.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police requests the Government of Canada to amend section 183 of the Criminal Code to include additional designated offences such as: Criminal Negligence Causing Death; Criminal Negligence Causing Bodily Harm; Manslaughter; Criminal Harassment ; Removal of a Child from Canada; Torture; Insider Trading; Possession of a firearm knowing it's possession is unauthorized; Possession of a prohibited or restricted firearm with ammunition; and, all driving related offences involving death or bodily harm.

Resolution #04 – 2015

AMENDMENTS TO SECTION 183 of the CRIMINAL CODE

Background

Canadian police leaders, through their personnel and CACP committee membership have researched the deficiencies in s. 183 of the Criminal Code as it relates to offences for which an application for an authorization to intercept private communications may be made and an authorization issued, pursuant to s. 185/186. It is interesting to note that, should the suggested re-writing of Part VI actually occur, the manner in which offences under section 183 are identified may change from an itemized list to a more comprehensive, yet simple process of identifying criteria offences based on minimum sentencing. Perhaps any offence punishable by 5 years or more would automatically designated for the purpose of Part VI.

Section 183 does contain an extensive list of "offences" and it has expanded over the years in an effort to reflect new offences added to the Criminal Code and other Acts of Parliament. That said, there are still several offences that are conspicuously absent, and result in limitations to gather evidence in these investigations.

Below is the primary list of suggested criminal offences that should be included by the membership of the CACP Law Amendments Committee:

1) Criminal Negligence Causing Death s. 220 Criminal Code
2) Criminal Negligence Causing Bodily Harm s. 221 Criminal Code
3) Manslaughter s. 236 Criminal Code
4) Criminal Harassment s. 264 Criminal Code
5) Torture s. 269.1 Criminal Code
6) Insider Trading s. 382.1 Criminal Code (Fraudulent Manipulation of the Stock exchange s. 380 is a designated offence. Insider Trading was later added to the Criminal Code but has been omitted in Part VI.)
7) All driving related offences involving death or bodily harm
8) Removal of a Child from Canada s. 273.3 of the Criminal Code.

There are also some firearms offences that are absent from s. 183:

9) Possession of a firearm knowing it's possession is unauthorized s. 92 Criminal Code
10) Possession of a prohibited or restricted firearm with ammunition s. 95 Criminal Code

Resolution #05 - 2015

RESOLUTION FOR THE SUPPORT OF THE CANADIAN COMMUNITY SAFETY INFORMATION MANAGEMENT STRATEGY (CCSIMS)

Submitted by the Information and Communications Technology Committee

WHEREAS the Canadian Association of Chiefs of Police (CACP) and its members have been sharing information since 1972 with the creation of the Canadian Police Information Centre (CPIC) and many other systems that followed, and;

WHEREAS the safety, security and prosperity of Canadians including law enforcement officers and their partners are reliant on the effective sharing of timely information, and;

WHEREAS numerous Canadian inquests, inquiries and studies have consistently identified the lack of information sharing and interoperability, both in relation to sharing between police organizations, and elements of the Justice system and other government and non –governmental organizations working toward public safety, as key barriers to successful and efficient investigative, operational and intelligence performance, and;

WHEREAS the Canadian Association of Chiefs of Police Information and Communications Technology Committee (previously known as the Informatics Committee) has been encouraging information sharing between law enforcement agencies and other public safety stakeholders since 1998 by hosting national conferences and leading advances such as the Police Information Portal, or PIP, which is managed by the National Police Service of the Royal Canadian Mounted Police, and;

WHEREAS in 2014 the ICT Committee, with funding from the Government of Canada's Centre for Security Science, completed a National Law Enforcement Information Management Study that clearly outlined the lack of interoperability between law enforcement information management systems in Canada and recommended the creation of a national strategy to improve information sharing, and;

WHEREAS the ICT Committee held a three day workshop in Ottawa in November 2014 with representatives from across Canada which resulted in the development of a draft Canadian Community Safety Information Management Strategy, and;

WHEREAS the Canadian Community Safety Information Management Strategy (CCSIMS) will benefit all Canadians by enhancing community safety and increasing efficiencies at the national level.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police supports the ongoing development of the Canadian Community Safety Information Management Strategy (CCSIMS) and its vision of getting the right information to the right people at the right time, and directs its Information and Communications Technology (ICT) Committee to continue to spearhead CCSIMS development, and;

BE IT FURTHER RESOLVED that the Canadian Safety and Security Program be requested to provide science and technology advice and resources in the continued development of CCSIMS.

Resolution #05 - 2015

RESOLUTION FOR THE SUPPORT OF THE CANADIAN COMMUNITY SAFETY INFORMATION MANAGEMENT STRATEGY (CCSIMS)

Background

The current law enforcement environment in Canada lacks a national governance or coordination body with federal, provincial, territorial, regional and municipal representation focused on information management. Information vital to a proper decision may exist in one system or may be fragmented over many silos of information. Funding for information management initiatives is fragmented, with no sustainable funding model in place.

There is limited sharing of information between police agencies and other community safety partners. The Hub Model, piloted in Saskatchewan has proven to be an excellent community safety practice with the potential to be a national model. However, attitudes toward sharing vary greatly from jurisdiction to jurisdiction and many times other members of public safety are fearful of sharing and do not fully recognize the value of such an approach[1]. At times this is due to privacy legislation that varies across jurisdictions and hampers efforts to improve information sharing. Today there is limited legislation in place that reflects a multijurisdictional approach to information sharing in support of community safety

Current data systems do not easily share information. To compound this, information retention and archiving practices vary across Canada. Major and national systems are in place but are not optimized for sharing. Although the US based National Information Exchange (NIEM) Model has been adopted within Canada, virtually no Requests for Proposal demand that this standard be used for data exchanges. It would make sense that basic NIEM functionality be requested in every RFP within public safety to move along the adoption process.

To make matters more complex, the full impacts of 700 MHz Broadband/LTE and Next Generation 9-1-1 are not clearly understood. For example, broadband technologies could supply an officer with all of the relevant information that could assist in a given situation, but in so doing there is a risk of information overload for the officers and other community safety partners. Defining what is important and relevant to an officer will require much work.

The purpose of the CCSIMS is to establish the framework and supporting Action Plan required to achieve the CCSIM Vision: "Responsible Information Management for Community Safety".

The sustainability of the cost of public safety is being debated and crime continues to evolve. In the evolution of policing and community safety strategies, information management is a key component. An enhanced Canadian Community Safety Information Management Strategy will allow all key community safety partners and services to work smarter and safer. If police

[1] As an example, in one case a person fell and struck his head coming out of a establishment where alcohol was served. He was taken to hospital, assessed and released into police custody for other reasons. The hospital would not supply any information on his condition citing privacy concerns. The person later died in cells. While it cannot be said that information sharing would have saved his life, it may have contributed to a better understanding of how to identify a deteriorating condition.

services manage their information effectively at a national level, the opportunities for increased efficiency, increased public safety, and officer safety will be fully realized.

By connecting the dots, the CCSIMS will lead to the development of the required components to support greater collaboration between services, which contribute to community safety. CCSIMS will allow for greater information management and sharing which in turn will enhance police service delivery in Canada. The result will be greater localized public safety knowledge and broader community partnerships.

The Canadian Community Safety Information Management Strategy (CCSIMS) aligns with the Communications Interoperability Strategy for Canada[2] and will be enabled by the following key elements:

- effective governance;
- a responsible sharing culture among public safety organizations;
- supporting and balanced legislation for sharing information;
- established and implemented National Data Standards and supporting standards-based approaches, procedures and processes; and
- technology enablers for responsible information management for community safety.

In simple terms, the CCSIM Strategy is designed to leverage people, processes and technology to get the right information to the right people at the right time in support of a broad community safety information sharing environment.

[2] The Communications Interoperability Strategy for Canada (CISC) is a strategic document that sets goals and identifies key national priorities to enhance governance, planning, technology, training and exercises to promote interoperable voice and data communications. The CISC, through its Action Plan, provides a series of action items, including milestones, to help emergency responders and relevant government officials make measurable improvements in day-to-day operations, as well as emergency communications, on an annual basis.

Resolution #06 - 2015

SUSTAINABLE FUNDING OF THE PUBLIC SAFETY CANADA ELECTRONIC CATALOGUE AND DIGITAL PORTAL FOR CANADIAN POLICE RESEARCH

Submitted by the CACP Research Foundation

WHEREAS the goal of the CACP Research Foundation is to create and develop the highest standards of effectiveness in law enforcement by fostering and encouraging research, and;

WHEREAS Public Safety Canada has made a valuable contribution to this goal by initiating work on two important research tools for police leaders – an electronic catalogue of Canadian police research and a digital portal through which research activities can be shared, and;

WHEREAS Canadian police leaders are expected to rely on research to make informed, evidence-based decisions, and;

WHEREAS police, researchers, academics, government at all levels, and others need access to Canadian police research in order to ensure police leaders are able to make evidence-based decisions, and;

WHEREAS the Public Safety Canada electronic catalogue and digital portal provide unprecedented access to Canadian police research and research activities, and;

WHEREAS funding and support for these tools has been confirmed through to February 2016, but not beyond, and;

WHEREAS further funding commitments are required beyond February of 2016 to ensure these tools are available, and sufficient staff are in place, to sustain the ongoing operations of the services provided by this important Public Safety Canada initiative.

THEREFORE BE IT RESOLVED that the Minister of Public Safety Canada be called upon to allocate sustainable funding to the electronic catalogue and digital portal in order to ensure police leaders are able to make evidence-based decisions that will improve public safety for Canadians.

Resolution #06 - 2015

SUSTAINABLE FUNDING OF THE PUBLIC SAFETY CANADA ELECTRONIC CATALOGUE AND DIGITAL PORTAL FOR CANADIAN POLICE RESEARCH

Background

Policing in Canada is changing. As the composition of society evolves, policing must evolve to meet increasingly complex needs. Today's police leaders are increasingly held accountable to governments and the public; they need and are expected to draw on relevant, evidence-based research to make informed decisions.

The CACP Research Foundation aims to create and develop the highest standards of effectiveness in law enforcement by fostering and encouraging research in to a variety of strategic and operational policing issues. In 2013, the CACP Research Foundation Board of Directors identified a need for an open and searchable catalogue of Canadian police research to ensure police leaders have the right tools to make evidence-based decisions. Concurrently, the Economics of Policing and Community Safety Shared Forward Agenda recognized the need for a central repository to improve access to policing research in Canada.

Public Safety Canada stepped forward with an offer to create an electronic catalogue of Canadian police research and a digital portal through which research activities can be accessed and shared. The Canadian Policing Research Catalogue was established in March 2015 in partnership with the Canadian Association of Chiefs of Police Research Foundation, the Canadian Police Association, the Canadian Association of Police Governance, and provincial and territorial government partners.

Today, the Canadian Policing Research Catalogue and digital portal are a consolidated online, searchable library of over 8000 titles of policing research that provides the policing community, policy makers, academics, other stakeholders and the public with a virtual online forum to access evidence-based policing research, information and best practices.

The library continues to receive and process research contributions from academics, police services and government agencies and addresses a wide variety of strategic and operational issues facing policing today. It is critical that funds be in place to ensure sufficient staff and tools are available to ensure the growth and on-going sustainability of these important tools.

Resolution #07 - 2015

CYBER CRIME: POLICE ROLES & RESPONSIBILITIES WITHIN A COLLABORATIVE NATIONAL FRAMEWORK

Submitted by Norm Taylor, Program Director, CACP Executive Global Studies Program

WHEREAS as proposed in Resolution #03 – 2012, and through the continuing work of the e-Crimes Committee, the CACP has called on the Government of Canada, together with its public and private sector partners to develop a National Cybercrime Strategy to disrupt cybercrime, and;

WHEREAS in August 2014, the CACP Board of Directors further recognized cyber crime as an emerging concern stating, it is "a topic that challenges the traditional skills, capacities, roles and response patterns of policing … the need for a coherent national response is an emerging priority for police leaders", and;

WHEREAS current empirical evidence suggests that solutions to cyber-based victimization demand effective collaboration among multiple actors, and that all levels of policing share unique responsibilities to protect citizens and to uphold the rule of law, and;

WHEREAS the CACP Global Executive Studies Program 2015 was directed by the CACP Board to research and illuminate a way forward for Canada on cyber crime by studying approaches in selected key countries to identify the most effective roles for police within such a collaborative framework, and;

WHEREAS in May 2015, after research and field interviews with almost 100 experts in nine countries representative of policing, government, academia, and private industry, the Global Studies cohort concluded that the most promising law enforcement responses to cyber crime are characterized by:

(1) Addressing cyber crime as a core policing matter
(2) Identifying cyber crime as a current community safety priority
(3) Recognizing that despite its complexity, cyber crime is actionable to some degree at all levels of policing, and;

WHEREAS the experience of other countries, combined with emerging domestic analysis, confirmed that the patterns of victimization, growing harm to communities, and threats to the rule of law, all fueled further by continued and rapid technological advances, argue urgently for a deliberate, coherent and sustained response by police services at all levels in Canada, and;

WHEREAS the CACP and its members, through adoption of this resolution, acknowledge that all "cyber crime", regardless of its underlying motivations, sources or forms, is in fact a crime; and, like all crime, it creates victims who merit our support. Notwithstanding the complexity and the need for broad collaborative strategies that must extend national capacity well beyond policing alone, all levels of police agencies continue to bear an obligation, to the extent of their capacity, to prevent cyber crime, to pursue cyber criminals and to protect their communities.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police calls on its partners, their associations, and FPT stakeholders to work with the CACP to accelerate the advancement and adoption of a consolidated National Cyber Crime Strategy, as envisioned in Resolution #03-2012, including frameworks, mechanisms and a structure to achieve better national coordination within law enforcement, and among law enforcement, government, academia and the private sector, and;

BE IT FURTHER RESOLVED that the Canadian Association of Chiefs of Police calls on the Federal Government to increase the focus on cyber crime**,** in line with the principles above, when it next updates "Canada's Cyber Security Strategy (2010)", and;

BE IT FURTHER RESOLVED that the Canadian Association of Chiefs of Police calls on its partners, their associations, and FPT stakeholders to collectively advocate for legislative, regulatory and policy change that will increase investigative efficiency and effectiveness, create greater risk and consequences for offenders, and more effectively facilitate the work of police in several areas, including but not limited to: reporting requirements; data preservation standards; MLAT reforms; domestic production orders for foreign data; modernized lawful access; and, extra-territoriality for certain vital cyber systems.

Resolution #07 - 2015

CYBER CRIME: POLICE ROLES & RESPONSIBILITIES WITHIN A COLLABORATIVE NATIONAL FRAMEWORK

Background

The CACP Executive Global Studies 2015 cohort was assigned the research theme of cyber crime, by the CACP Board of Directors. After completing a nine-country comparative study, preceded by domestic research and the development of a comprehensive baseline for Canada, the CACP Global team has made several notable observations and findings on the comparative state of current police roles in this important and growing issue in Canada. These findings will form the basis of a presentation to members at the Annual Conference in August, 2015, a report to the Board, and a number of other communication products currently being produced by the team.

Generally speaking, Canada is currently behind the curve in almost all aspects of cyber resilience and response. There are several examples where this is being addressed with increasing priority, and a growing number of partners are becoming engaged. However, to date, much of this work has been focused on threats to national security, threats to the broader economy, threats to critical infrastructure, and threats to the private sector, including the financial sector. All of this work is important and CACP Global is calling attention to the need to accelerate the adoption of the "Canada's Cyber Security Strategy (2010)" as outlined in this resolution.

What is most notably lacking in Canada, by comparison to other jurisdictions, is any kind of comprehensive appreciation, focus or broadly based response to *cyber crime* across the policing system, and especially its associated threats to community safety. Under reporting of cyber incidents is in the extreme. In fact, several of our police services have been victims of cyber attacks, and even some of these incidents have not been reported or documented as 'crimes'. CACP Global believes that much of this is due to several factors, notably a lack of knowledge among police, a lack of recognition of the strategic importance of linking cyber activity to community safety priorities, and an under-appreciation of the patterns and impacts of victimization of our citizens.

Among the wide array of actors who must play various roles in a collaborative response to malicious cyber activity in all its forms, our police system holds some very unique responsibilities when it comes to cyber crime, among them ensuring the protection of citizens at the local level, building greater resilience in our communities, providing adequate support to victims, deterring criminal behaviour by raising the risks and consequences for offenders, and ensuring proper applications of the criminal justice system to uphold the rule of law.

All cyber crime is crime. And all crime creates victims. While recognizing the continuing importance of broad, collaborative responses that will extend well beyond the capacities of the average police service, CACP Global believes it is nonetheless vital and urgent that Canadian policing must get into this game.

Resolution #08 - 2015

AMENDMENTS TO THE CANADA POST CORPORATION ACT

Submitted by the Law Amendments Committee

WHEREAS the *Canada Post Corporation Act* currently provides that "nothing in the course of post is liable to demand, seizure, detention or retention",[3] and;

WHEREAS Canadian Police Leaders are concerned that contraband is being sent through the mail system with impunity from judicially authorized search or seizure. By way of example, based on information contained in a censored version of the RCMP's November 2012 "Postal Assessment 2012" prepared for the Canadian Association of Chiefs of Police's Organized Crime Committee, these reports exposed cases in which guns, grenades, a rocket launcher, stun guns, dangerous chemicals, and drugs such as cocaine, heroin and marihuana were shipped through the postal system.[4] These items represent a significant threat to postal workers and Canadians, and;

WHEREAS this represents a significant challenge for Canadian law enforcement, as reliable intelligence and information that points to contraband being moved through the mail system may not be acted upon by police until it is successfully delivered. This forces law enforcement to find alternative ways to work within or around the Canada Post system and legislative framework in order to apprehend criminals who use the postal system as a way to move various forms of contraband including weapons, illicit drugs and counterfeit items across Canada, and;

WHEREAS there is an ongoing need to amend the *Canada Post Corporation Act* in order that Canada Post and the Canadian law enforcement community develop ways to effectively work together to stop the transmittal of contraband through the postal system, and;

WHEREAS the Canadian Association of Chiefs of Police, as the national voice of Canadian police leadership, is committed to raising issues where federal legislation, such as the *Canada Post Corporation Act*, should be amended.

THEREFORE BE IT RESOLVED that the Canadian Association of Chiefs of Police requests the Government of Canada to amend the *Canada Post Corporation Act* to provide police, for the purpose of intercepting contraband, with the ability to obtain judicial authorization to seize, detain or retain parcels or letters while they are in the course of mail and under Canada Post's control.

---

[3] Section 40 (3) - Subject to the *Canadian Security Intelligence Service A*ct, the *Customs Act* and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*

[4] http://news.nationalpost.com/2013/09/18/criminals-using-canada-post-to-transport-illicit-goods-including-a-rocket-launcher-rcmp-report-says/
http://www.thestar.com/news/canada/2013/09/17/guns_grenades_drugs_counterfeit_goods_arrive_by_canada_post.html

Resolution #08 - 2015

AMENDMENTS TO THE CANADA POST CORPORATION ACT

Background

Canadian police leaders, through their personnel and CACP committee membership have identified the deficiencies in the *Canada Post Corporation Act* as it relates to seizure powers of law enforcement while items are in transit in the postal system, also referred to as "during the course of post".

By way of example, on an annual basis, the RCMP and CBSA partner together in a week long INTERPOL operation to disrupt the online sale of counterfeit and unlicensed medicine. The 2013 enforcement initiative netted some 238,820 illicit and fake medicines including antibiotics, hormone replacement, muscle relaxants, erectile dysfunction pills, weight loss pills, beta blockers and bronchodilators. These medicines were worth $1,032,514 and came from 3,223 packages originating in 19 countries, while raids across the globe resulted in the seizure of 9,800,000 illicit medicines worth 41,000,000 USD. This highlights a global trend in which postal and courier systems are used to move contraband across international borders.[5]

The issue of contraband being sent through the mail has also become known in Canadian society. In September 2013, it was reported by the media that the Canadian postal system is being used to transmit various forms of contraband, including illicit drugs, weapons and counterfeit items. Based on information contained in a censored version of the RCMP's November 2012 "Postal Assessment 2012" prepared for the Canadian Association of Chiefs of Police's Organized Crime Committee, these reports exposed cases in which guns, grenades, a rocket launcher, stun guns, dangerous chemicals, and drugs such as cocaine, heroin and marihuana were shipped through the postal system.[6] These items represent a significant threat to postal workers and Canadians.

The *Canada Post Corporation Act* (CPCA) is the legislative basis for the Canada Post Corporation and was passed in 1981. Subject to the *Canadian Security and Intelligence Service Act*, the *Customs Act* and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, the *Canada Post Corporation Act* currently exempts items in the course of post from search or seizure by law enforcement, pursuant to the *Criminal Code*, *Controlled Drugs and Substances Act*, *Copyright Act* or *Trade-marks Act*[7], and potentially others. This exclusion may perhaps be due to domestic trafficking not being seen as a priority when section 40(3) of the CPCA was last updated in 2005. This means that search and seizure authorities granted to law enforcement personnel under the *Criminal Code of Canada* or other criminal law authorities are overridden by the CPCA, giving law enforcement no authority to seize, detain or retain parcels or letters while they are in the course of mail and under Canada Post's control. That said, the CPCA is augmented by the *Non-mailable Matter Regulations* which specify that Canada Post inspectors

[5] http://www.rcmp-grc.gc.ca/news-nouvelles/2013/06-27-pangea-eng.htm
http://www.interpol.int/News-and-media/News-media-releases/2013/PR077
[6] http://news.nationalpost.com/2013/09/18/criminals-using-canada-post-to-transport-illicit-goods-including-a-rocket-launcher-rcmp-report-says/
http://www.thestar.com/news/canada/2013/09/17/guns_grenades_drugs_counterfeit_goods_arrive_by_canada_post.html
[7] *Canada Post Corporation Act*, Section 40(3)

shall turn over any illegal material found in the course of mail to law enforcement. Recent court rulings have determined that postal inspectors cannot act as agents of the state where police convey information received to postal inspectors in order to intercept the contraband during the postal delivery process.

This represents a significant challenge for Canadian law enforcement, as reliable intelligence and information that points to contraband being moved through the mail system may not be acted upon by police until it is successfully delivered. This forces law enforcement to find alternative ways to work within or around the Canada Post system and legislative framework in order to apprehend criminals who use the postal system as a way to move various forms of contraband including weapons, illicit drugs and counterfeit items across Canada.

It is imperative that Canada Post and the law enforcement community develop ways to effectively work together to stop the transmittal of contraband through the postal system.

The CACP Drug Committee and the CACP Law Amendments Committee have jointly discussed the issue and concluded that the *Canada Post Corporation Act* requires legislative amendments in order to fully address law enforcement's concerns.