Evaluation of the Investigative Powers for the 21st Century Initiative

Final Report

March 2020

Evaluation Branch
Internal Audit and Evaluation Sector

Department of Justice Canada | Ministère de la Justice Canada

Canada

ACKNOWLEDGEMENT

The Chief Audit and Evaluation Executive would like to thank the evaluation team and those individuals who contributed to this engagement and particularly, employees from the Department of Justice Canada, Public Prosecution Service of Canada, the Royal Canadian Mounted Police, and Global Affairs Canada, who provided insights and comments as part of this evaluation.

ACRONYMS

BSI	Basic Subscriber Information
Budapest Convention	*Convention on Cybercrime of the Council of Europe*
Charter	*Canadian Charter of Rights and Freedoms*
CLPS	Criminal Law Policy Section (Justice)
CSP	Communications Service Provider
EC3	European Crime Centre (Europol)
EU	European Union
FBI	Federal Bureau of Investigation (U.S.)
GAC	Global Affairs Canada
GOC	Government of Canada
IAG	International Assistance Group (Justice)
IOCTA	Internet Organised Crime Threat Assessment
IP21C	Investigative Powers for the 21st Century
IP	Internet Protocol
ISP	Internet Service Provider
J-CAT	Joint Cybercrime Taskforce
JLA	Criminal, Security and Diplomatic Law Division, Legal Affairs Bureau (GAC)
Justice	Department of Justice Canada
LSU	Legal Services Unit
MLA	Mutual Legal Assistance
MLACMA	*Mutual Legal Assistance in Criminal Matters Act*
NC3	National Cyber Crime Coordination Unit (RCMP)
NCECC	National Child Exploitation Crime Centre (RCMP)
OAS	Organization of American States
PCOCA	*Protecting Canadians from Online Crime Act*
PPSC	Public Prosecution Service of Canada
RCMP	Royal Canadian Mounted Police
TechOp	Technical Operations (RCMP)
T-CY	Cybercrime Convention Committee (Council of Europe)
TDR	Transmission Data Recorder
TIS	Technical Investigative Services (RCMP)
TSP	Telecommunications Service Provider

TABLE OF CONTENTS

List of Tables

List of Figures

EXECUTIVE SUMMARY

Introduction

This report presents the results of an evaluation of the *Investigative Powers for the 21st Century Initiative* (IP21C), a horizontal initiative led by the Department of Justice Canada (Justice) in collaboration with the Public Prosecution Service of Canada (PPSC), the Royal Canadian Mounted Police (RCMP) and Global Affairs Canada (GAC).

The IP21C Initiative has supported the implementation of new legal authorities arising from former Bill C-13, the *Protecting Canadians from Online Crime Act* (PCOCA) that came into force on March 10, 2015.

Program Description

It had long been recognized that new investigative powers were needed both to protect Canadians and investigate crimes that are facilitated by computer and communications technology, and to combat crimes that have a transnational dimension.

Since 2000, the Government of Canada (GOC)'s efforts through the Lawful Access Initiative (LAI) have concentrated on assessing the need for new and amended legislation. The IP21C Initiative stems from the portions of the LAI relating to amendments to the *Criminal Code*, which came into force with the enactment of the PCOCA. This Act introduced specialized investigative powers under judicial authorization to obtain digital evidence. It amended the *Criminal Code*, the *Mutual Legal Assistance in Criminal Matters Act* (MLACMA), the *Canada Evidence Act* and the *Competition Act* which:

- added to the regime of production orders to provide more precise tools to respond to contemporary technology and related investigative requirements while balancing privacy and human rights appropriately;
- introduced a new regime for rapidly preserving volatile data, using preservation demands and orders;
- supported the gathering of digital evidence in criminal investigations, including to assist foreign investigative and prosecution authorities; and,
- enabled Canada to ratify the Convention on Cybercrime of the Council of Europe (the Budapest Convention), which occurred on July 8, 2015. The Convention is the only multilateral-level legal instrument to combat computer-related crime.

The IP21C Initiative was supported by funding of $60.74 million over five years (2015-16 to 2019-20) and ongoing funds of $12.25 million annually.

Justice, PPSC, the RCMP and GAC are jointly responsible for managing the implementation of the IP21C Initiative, while each executes its specific activities in the criminal justice and international policy systems. The primary target populations for the IP21C Initiative are police and prosecutors. The intent is to provide them with more effective means to investigate and prosecute cybercrime and computer-assisted crime, while respecting the privacy and freedoms of Canadians.

Five main activities have been implemented by the Initiative:

- **Legal analysis, policy development and coordination on domestic and international issues** – Includes legal and policy advice, litigation support and prosecution services required to steward implementation of the legislative provisions related to investigative powers in the PCOCA, as well as to meet Canada's international obligations stemming from ratification of the Budapest Convention.

- **Awareness and training** – Includes development of awareness and training materials to ensure that the legislative reforms enacted by the PCOCA would be implemented in a consistent manner. The primary audiences for training have been the law enforcement community and prosecutors. Efforts were also directed at raising awareness of the PCOCA provisions among Canada's international partners.

- **Technical research and tools to support criminal investigations** – Involves the development of new tools, techniques and solutions for warranted, real time interception of transmission data and analysis of seized data, including international requests related to the Budapest Convention.

- **Administration of a data preservation scheme** – Involves developing a dedicated triage function to administer a new data preservation scheme, in accordance with the legal provisions in the PCOCA, and to respond to international requests for assistance.

- **International cooperation** – Involves advancing international cooperation on cybercrime and ensuring that Canada's interests related to cybercrime and other computer-assisted crimes are reflected in Canada's broader foreign policy.

Findings

The main findings of the horizontal evaluation of the IP21C Initiative with respect to the evaluation issues are summarized below.

Relevance

The overall objective of the IP21C Initiative – to provide the means to implement the investigative powers added to the *Criminal Code* by the PCOCA and to meet Canada's international obligations stemming from ratification of the Budapest Convention – continues to be relevant, as cybercrime and computer-assisted crimes are growing at a fast rate both in Canada and internationally, and criminals are increasingly exploiting evolving technologies.

The PCOCA provided legislative reforms that were necessary to permit specialized investigative powers under judicial authorization to obtain digital evidence not only for the high-tech computer crimes such as hacking, or organized crime, but also to deal with everyday offences when a criminal sends an email, uses their cell phone, or posts an image on a social networking site. These reforms have led to a regime of production orders that enable a judge to know precisely what type of data is being sought and to balance privacy and human rights. Additionally, the PCOCA introduced a new regime for rapidly preserving volatile data, using preservation demands and preservation orders.

The evaluation evidence indicates that there is an ongoing need for the key activities funded by the IP21C Initiative, including:

- **Legal analysis, policy development and coordination on domestic and international issues –** While there has been very little litigation with respect to the IP21C investigative powers to date and no successful *Charter of Rights and Freedoms (Charter)* challenges, Justice needs to maintain the capacity to defend any future challenges and to make future

amendments to the *Criminal Code* as required. GAC also needs to continue to coordinate Canada's foreign policy approach on cybercrime in the international arena, which is becoming increasingly complex and politicised.

- **Awareness and training –** The "awareness" phase of the IP21C Initiative has ended, as prosecutors and law enforcement are now very familiar with the IP21C-related investigative powers. Outreach activities will need to continue to assist stakeholders in applying the *Criminal Code* provisions, primarily on a reactive or as needed basis. Ongoing training of prosecutors and law enforcement officials on the *Criminal Code* amendments has become integrated into the training programs offered by such organizations as the Canadian Police College and the PPSC School for Prosecutors.

- **Administration of data preservation scheme –** The IP21C Initiative has enabled the RCMP to develop and implement a data preservation scheme to handle a large volume of data preservation requests from foreign law enforcement. This activity needs to continue, as Canada will continue to receive preservation requests from foreign law enforcement and therefore must maintain a capability to manage such requests. The RCMP established a National Cyber Crime Coordination Unit to be a single point of contact.

- **Technical research and tools to support criminal investigations –** RCMP Technical Investigations Services have developed tools to access, obtain and process digital evidence from a device or digital storage medium seized as evidence (data at rest) as well as tools that are deployed in a live communications situation (data in motion). As cybercrimes are becoming increasingly more technologically complex, it will be critical for the RCMP and other federal agencies to develop additional tools to support criminal investigations.

Moreover, the Budapest Convention is the main international instrument on cybercrime. It aims to help its state parties to harmonize their national laws, improve their investigative techniques, and increase cooperation. Ratification of the Convention allowed Canada to cooperate with other signatory countries in the investigation of cybercrime and enabled access to digital evidence that may be found in another country. Canada is viewed as playing a strong role internationally in supporting the Convention.

While the evidence from this evaluation indicates that the PCOCA addressed a significant need to modernize the investigatory powers in the *Criminal Code*, Canada's laws need to continually evolve so that law enforcement and prosecutors are equipped with the tools necessary to combat cybercrime and other computer-assisted crime. Police and prosecutors highlighted in particular the challenges associated with obtaining timely access to basic subscriber information and encrypted data.

Performance

The findings of the evaluation regarding the performance of the IP21C Initiative in achieving its main intended outcomes are as follows:

- **Awareness and knowledge of the IP21C-related investigatory powers** – The target audiences of the IP21C Initiative, including law enforcement, prosecutors and telecommunications service providers are now very familiar with the legislative amendments made to the *Criminal Code* and other acts. IP21C officials devoted considerable effort to raising awareness and knowledge of the key elements of the PCOCA.

- **Management of issues and consistency of implementation and interpretation of the investigatory powers** – Relatively few legal and operational issues have arisen related to the new investigatory powers. While it was expected that numerous *Charter* challenges would arise from the new investigative powers, this has not yet proved to be the case. The resources

provided to the federal partners by the IP21C Initiative have helped them to manage implementation of the investigatory powers in a variety of ways, ranging from supporting prosecutions that rely on these powers to providing internal stakeholders with legal and policy advice. The main legal issue raised by key informants is that the new transmission data recorder warrant provisions do not provide access to basic subscriber information. The investigatory powers have largely been consistently implemented across Canada.

- **An improved ability to combat cybercrime and computer-assisted crime** – The IP21C Initiative has contributed to improving Canada's operational ability to combat cybercrime and other computer-assisted crimes, both domestically and internationally. IP21C officials have collaborated extensively with each other and with external stakeholders to support implementation of the IP21C-related investigatory powers. The RCMP has implemented a dedicated triage function to process and track data preservation requests received from foreign law enforcement. It also has developed new tools to access, obtain and process digital evidence from devices seized as evidence, as well as tools used in a live intercept situation.

- **Improved international co-operation to obtain digital evidence** – The IP21C Initiative has helped Canada to increase its level of cooperation internationally to obtain digital evidence to combat cybercrime and computer-assisted crime. Canada is viewed by international stakeholders as being in compliance with its requirements under the Cybercrime Convention and other applicable mutual legal assistance (MLA) agreements. Canada is viewed internationally as playing an important role in supporting the Convention, with a considerable effort devoted to the drafting of a Second Additional Protocol, still under negotiation within the Council of Europe. Justice IAG has improved the speed with which MLA requests seeking digital evidence received from foreign law enforcement and prosecutors are processed and executed. The Initiative also contributed to improved coordination and consistency in Canada's foreign policy approach on cybercrime and computer-assisted crime.

Design

The IP21C Initiative has been well coordinated. The IP21C Initiative business plan was thoroughly prepared and the Initiative has evolved as expected.

Recommendations

No recommendations are included as the IP21C Initiative was implemented as expected and there are no identified barriers to the achievement of expected results.

1. INTRODUCTION

1.1 Purpose of the Evaluation

This report presents the results of an evaluation of the *Investigative Powers for the 21st Century Initiative* (IP21C), a horizontal initiative led by the Department of Justice Canada (Justice) in collaboration with the Public Prosecution Service of Canada (PPSC), the Royal Canadian Mounted Police (RCMP) and Global Affairs Canada (GAC). The evaluation was conducted in accordance with the Treasury Board's *Policy on Results* (2016). The evaluation was undertaken by the Department of Justice Evaluation Branch between September 2018 and September 2019, as per the *2018-19 Departmental Evaluation Plan*.

1.2 Evaluation Scope

The evaluation examined the relevance, performance and design of the Initiative and covered the period following the enactment of Bill C-13, the *Protecting Canadians from Online Crime Act* (PCOCA), on March 10, 2015 up to March 31, 2019. The initial year, 2015-16, was treated as the baseline as the federal partners (IP21C officials) began to hire staff and implement the various funded activities. This also was the year in which Canada ratified the Budapest Convention (on July 8, 2015).

2. PROGRAM PROFILE

Evolving computer and communications technologies have changed the way Canadians communicate and live their lives. They may use multiple communication devices and a wide variety of tools such as email, instant messaging and various social media applications. While this evolution provides enormous benefits for Canadian society, criminals are using the same technologies for illicit purposes. Digital communications are now a fundamental tool for virtually all criminal activity, and digital information is sometimes more important than physical evidence or intelligence in investigating and prosecuting crimes.[1]

It has long been recognized that Canada's law enforcement must be able to work as effectively in the digital world as they do in the physical. They must also have the capability to cooperate with their international partners who seek digital evidence from Canada to support their criminal investigations and prosecutions. The laws governing the collection of information and evidence needed to be updated to reflect the advancements of digital technology that began during the latter part of the twentieth century.

The Government of Canada's (GOC) Lawful Access Initiative (LAI) provides a framework for the development of technical solutions and legislative options. Lawful access is an important and well-established technique used by law enforcement in the prevention and investigation of serious offences. It consists of the interception of communications and the search and seizure of information conducted under lawful authority. Since 2000, the GOC's efforts through the LAI have concentrated on assessing the need for new and amended legislation. The Government's approach to lawful access recognizes the need for effective measures that balance rights, privacy, safety, security and economic well-being of all Canadians. To realize their public safety mandate, law enforcement and national security agencies need to maintain their lawful access capabilities in a manner that continues to respect the

[1] Government of Canada, *Our Security, Our Rights: National Security Green Paper, 2016, Background Document*, 2016, p. 54, retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-en.pdf

Charter. In the 2001 Speech from the Throne[2], the Government pledged to provide modern tools to deal with cybercrime and to update the existing legal framework in order to help law enforcement and national security agencies address the challenges posed by advanced communications and information technologies.[3]

The IP21C Initiative stems from the portions of the LAI relating to amendments to the *Criminal Code*, which came into force in March 2015 with the enactment of the PCOCA. This Act introduced specialized investigative powers under judicial authorization to obtain digital evidence. It amended the *Criminal Code*, the *Mutual Legal Assistance in Criminal Matters Act* (MLACMA), the *Canada Evidence Act* and the *Competition Act* which:

- added to and/or improved the regime of Canadian search warrants and production orders[4] to provide more precise tools to respond to contemporary technology and related investigative requirements while balancing privacy and human rights appropriately;
- introduced a new regime for rapidly preserving volatile data, using preservation demands and orders[5];
- supported the gathering of digital evidence in criminal investigations; and,
- enabled Canada to ratify the Budapest Convention, which, as noted above, occurred on July 8, 2015. The Convention is the only international-level legal instrument to combat computer-related crime.

Key Definitions

*A **search warrant** provides judicial authorization to law enforcement agencies to search and seize information.*

*A **production order** is a judicial authorization that compels the custodian of the information (e.g. internet service provider) to provide the information to a law enforcement agency.*

*A **preservation demand or order** directs a person, such as an internet service provider, to preserve computer data that are in their possession or control.*

The main purpose of the IP21C Initiative is to provide the means to implement the amendments made to the *Criminal Code* and the other Acts by the PCOCA and to meet Canada's international obligations, including those stemming from the ratification of the Budapest Convention. The PCOCA also introduced sanctions for Telecommunications Service Providers (TSPs) that do not comply with production demands and orders. The Initiative's overall goal is to help ensure that the GOC achieves its commitments to protect Canadians from cybercrime and to provide a solid legal framework with respect to all crimes that involve digital evidence – in a manner consistent with the *Charter*.

Justice, PPSC, the RCMP and GAC are jointly responsible for managing its implementation, while each executes its specific activities in the criminal justice and international policy systems. The logic model for the Initiative, which illustrates the relationship between the planned activities and its expected results, can be found in Appendix A. The Initiative consists of five main activities as follows:

---

[2] Government of Canada, Speech from the Throne to open the First Session Thirty-Seventh Parliament of Canada, 2001, retrieved from https://lop.parl.ca/sites/ParlInfo/default/en_CA/Parliament/procedure/throneSpeech/speech371
[3] Department of Justice Canada, *Lawful Access – Consultation*, 2002, retrieved from https://www.justice.gc.ca/eng/cons/la-al/index.html
[4] For further information, see: Library of Parliament, *Legislative Summary: Bill C-13: An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, Publication No. 41-2-C13-E, retrieved from https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/LegislativeSummaries/PDF/41-2/c13-e.pdf
[5] Ibid.

- **Legal analysis, policy development and coordination on domestic and international issues** – Includes legal and policy advice, litigation support and prosecution services required to steward implementation of the legislative provisions related to investigative powers in the PCOCA, as well as to meet Canada's international obligations stemming from ratification of the Budapest Convention.

- **Awareness and training** – Includes development of awareness and training materials to ensure that the legislative reforms enacted by the PCOCA are implemented in a consistent manner. The primary audiences for training are the law enforcement community and prosecutors. Efforts were also directed at raising awareness of the PCOCA provisions among Canada's international partners.

- **Technical research and tools to support criminal investigations** – Involves the development of new technical tools, techniques and solutions for warranted, real time interception of transmission data and analysis of seized data, including international requests related to the Budapest Convention.

- **Administration of a data preservation scheme** – Involves developing a dedicated triage function to administer a new data preservation scheme, in accordance with the legal provisions in the PCOCA, and to respond to international requests for assistance.

- **International cooperation** – Involves advancing international cooperation on cybercrime and ensuring that Canada's interests related to cybercrime and other computer-assisted crimes are reflected in Canada's broader foreign policy.

The primary target populations for the IP21C Initiative are police and prosecutors. The intent is to provide them with more effective means to investigate and prosecute cybercrime and computer-assisted crime, while respecting the privacy and freedoms of persons in Canada. A description of the roles and responsibilities of each partner, as well as additional information regarding the IP21C Initiative, are included in Appendix A.

The IP21C Initiative received funding in the amount of $60.74 million over five years (2015-16 to 2019-20) and ongoing funds of $12.25 million annually. Table 1 presents an overview by department of the funding, consisting of Vote 1 transfers for operating expenditures and an allocation for accommodation (13%). Given the nature of the work, the regular course of duties of most incumbents' positions includes work on cybercrime and computer-assisted crime as well as other related files, such as Lawful Access and Cyber Security. As such, expenditure data is not available because the resources are not always tracked separately. Based on information provided by IP21C officials, the majority of planned full-time equivalent positions have been staffed. Furthermore, as outlined throughout the findings, all of the planned activities have been implemented.

Table 1: IP21C Initiative Budget 2015-16 to 2019-20 ($)

Department	2015-16	2016-17	2017-18	2018-19	2019-20	Total
Justice	2,194,268	2,138,598	2,168,598	2,118,598	2,118,598	10,738,660
PPSC	4,426,717	4,121,778	4,127,237	3,998,804	3,998,804	20,673,340
RCMP	4,793,580	4,775,210	5,542,300	5,485,650	5,485,650	26,082,390
GAC	650,000	650,000	650,000	650,000	650,000	3,250,000
Total	**12,064,565**	**11,685,586**	**12,488,135**	**12,253,052**	**12,253,052**	**60,744,390**

Source: Program planning documents

The number of full-time equivalents (FTEs) allocated to each department, by year are presented below in Table 2.

Table 2: Allocated Full-Time Equivalent Staffing Overview

Department	2015-16	2016-17	2017-18	2018-19	2019-20	Ongoing
Justice	9.5	9.5	9.5	9.5	9.5	9.5
PPSC	22.0	21.5	21.5	20.8	20.8	20.8
RCMP	12.0	18.0	23.0	23.0	23.0	23.0
GAC	2.0	2.0	2.0	2.0	2.0	2.0
Total	**45.5**	**51.0**	**56.0**	**55.3**	**55.3**	**55.3**

Source: Program planning documents

3. EVALUATION METHODOLOGY

An interdepartmental Evaluation Working Group was established to support the evaluation by providing inputs, advice and suggestions regarding the design and conduct of the evaluation. The Working Group was established at the outset of the evaluation and included IP21C officials and representatives from evaluation units from each of the federal partner departments.

The methodology for this evaluation included multiple lines of evidence and employed the following data collection methods:

3.1 Document Review

The main internal documents reviewed included the following:

- IP21C Initiative Performance Measurement Strategy (April 2016).
- Fact sheets, PowerPoint decks and primers on the Bill C-13 legislative changes, prepared by the Criminal Law Policy Section (CLPS) and International Assistance Group (IAG), Justice.
- Documents related to the 2017 National Security consultations and 2018 National Cyber Security Strategy.

3.2 Review of Performance Information

As part of the Initiative's performance measurement strategy, IP21C officials compiled performance data associated with each of the intended outcomes. At the time of the evaluation, information was available for three years: 2015-16 to 2017-18 inclusive. This data was reviewed for the purposes of the evaluation.

3.3 Literature Review

A focussed literature review was undertaken of articles and reports that provide information on such topics as trends in cybercrime and challenges to law enforcement; Europol's annual Internet Organised Crime Threat Assessment (IOCTA); and assessment reports by the Council of Europe related to implementation of the Budapest Convention by Member States. In addition, an online search to identify court cases pertaining to the IP21C investigative powers between March 2015 and March 2019 was conducted and relevant case law was reviewed.

3.4 Review of Trends in Cybercrime and Computer-Assisted Crime

This review focussed on the collection and analysis of data on the incidence, investigation and resolution of two general categories of crime involving computer services:

- **Cyber-dependent crimes**: offences that can only be committed using computers, computer networks or the Internet, and target the computers and computer systems of individuals and organizations (also referred to as "technology-as-target" offences).

- **Cyber-enabled crimes**: "traditional" offences that are facilitated, or the reach and effects magnified, by the use of computers and the Internet (also referred to as "technology-as-instrument" offences).

Documents reviewed for this trends analysis related to the reporting of cybercrimes to police services in Canada, Eurobarometer surveys in Europe that included questions on cyber security incidents experienced by members of the public, and surveys of business organizations in Canada, and business and charitable organizations in England and Wales, regarding approaches to cybersecurity and cyber incidents.

3.5 Key Informant Interviews

A total of 36 key informant interviews were conducted, consisting of both internal and external key stakeholders. The breakdown is as follows:

- IP21C officials (headquarters and regions) from Justice, PPSC, RCMP and GAC. (24 interviews)

- Other GOC Departments with linkages to IP21C Initiative activities (Public Safety Canada and Innovation, Science and Economic Development Canada). (2 interviews)

- Domestic stakeholders (law enforcement and prosecution), including representatives from the law enforcement and provincial prosecution service communities (municipal and provincial police forces, provincial attorneys general). (3 interviews)

- Domestic stakeholders (other), consisting of major TSPs. (4 interviews)

- International stakeholders, consisting of justice officials in other countries (U.S.) and representatives of international entities (Europol, Council of Europe) where the IP21C Initiative has participated in working groups or consulted on issues related to cybercrime. (3 interviews).

In reporting the findings from the interviews, the following scale was used:

- A few: 10% to 15% or less

- Some: 15% to approximately 40%

- Many: more than 40% to approximately 60%

- Most: more than 60% to approximately 80%

- Almost all: more than 80%.

3.6 Limitations

The evaluation encountered a few methodological limitations or challenges, as discussed below by line of evidence.

Review of trends in cybercrime and computer-assisted crime. Many published surveys and estimates of the scale of cybercrime and its impacts are considered unreliable, incomplete, and/or inconsistent. In turn, these data weaknesses give rise to limitations in the evidence base to inform the development of cybercrime policies, response strategies and allocation of resources, not to mention the assessment of actions taken. Principal weaknesses and challenges identified in the literature reviewed include the following:

- Under-reporting of cybercrime incidents to the police and other authorities by individuals and organizations.
- Limited identification and differentiation of cyber-dependent or cyber-enabled incidents in crime reporting systems.
- Poorly designed survey methodologies for estimating victimization rates and impacts. The "gold standard" for measuring the incidence of cybercrimes is random probability sampling using a sufficiently large and stratified sample to obtain reliable representation, to enable the preparation of sound estimates of overall rates of cyber incidents and impacts.
- Other cybercrime surveys, particularly those published by providers of cybersecurity services and/or systems monitoring often lack transparency and consistency but do play a valuable role in identifying and characterizing emerging new cyber threats.
- The dynamic nature of cybercrime, in which the mechanisms used to carry out cybercrimes are continually evolving, meaning that responses by the authorities and measurement of the incidence and effects are always playing "catch-up".

Review of Performance Information. IP21C officials were able to provide performance information for the three years of implementation. However, it was challenging for the evaluation to assess the effectiveness of the awareness and training undertaken as part of the Initiative, as post-training evaluations had not been implemented at the time of the events. To address this, the evaluation used key informant interviews to collect this data. Though many of the key informants could not recall the specific training activities in which they participated, most were very familiar with the key elements of the PCOCA.

Key Informant Interviews. One limitation was the possibility of introducing bias as a result of the approach to sampling for the key informant interviews as well as the voluntary nature of participation in this data collection method. Self-reported response bias occurs when individuals are reporting on their own activities and may want to portray themselves in the best light. Strategic response bias occurs when the participants answer questions with the desire to affect outcomes. To alleviate this, the evaluation ensured that the list of key informants was balanced so that a knowledgeable pool of respondents and a variety of internal and external perspectives was gathered.

Mitigation Strategy. To mitigate these limitations, the evaluation used multiple lines of evidence and triangulation to confirm the results.

4. FINDINGS

4.1 Relevance

4.1.1 Ongoing Need for the IP21C Initiative

The overall objective of the PCOCA – to ensure that threats from cybercrime and computer-assisted crime are identified and acted upon – continues to be relevant, as cybercrime is growing at a fast rate both in Canada and internationally. The Initiative provides the means to implement the legislative reforms that created specialized investigative powers under judicial authorization to preserve and obtain digital evidence. Ratification of the Budapest Convention allows Canada to cooperate with other signatory countries in the investigation of cybercrimes.

As outlined in Section 2, the main purpose of the IP21C Initiative is to provide the means to implement the amendments made to the *Criminal Code* and the other acts by the PCOCA, and to meet Canada's international obligations stemming from ratification of the Budapest Convention. This is to help ensure that the GOC achieves its commitments to protect Canadians from cybercrime and provide a solid legal framework with respect to all crimes that involve digital evidence – in a manner consistent with the *Charter*.

Cybercrime continues to be a growing problem in Canada and around the world.[6] Annual data compilations by Statistics Canada for the four-year period from 2014 to 2017 show that the total number of reported cybercrime incidents rose from 15,184 in 2014 to 27,829 in 2017 – an annual compound growth rate of 22.4%.[7] Cyber-aided fraud accounted for close to half of all reported incidents in each year (47-48%), followed by production, distribution or possession of child pornography (13-17%), indecent/harassing communications and non-consensual distribution of intimate images (a new offence added to the *Criminal Code* by the PCOCA) (5-10%), uttering threats (6-7%) and criminal harassment (4-6%).[8]

Many of today's crimes involve criminals using cell phones or computers to send messages through the Internet using telecommunications capabilities. Unlike forensic evidence localized at a crime scene, digital evidence can be scattered across many devices at multiple locations sometimes in different jurisdictions. Moreover, electronic data can exist along a spectrum of permanence, from being very volatile and transient, existing for only a fraction of a second, to being archived, frozen in long-term secure storage. The PCOCA provided legislative reforms that were necessary to permit specialized investigative powers under judicial authorization to obtain digital evidence not only for the high-tech computer crimes such as hacking, or organized crime, but also to deal with everyday offences when a criminal sends an email, uses their cell phone, or posts an image on a social networking site. The reforms have led to a regime of production orders that enable a judge to know precisely what type of data is being sought and to balance privacy and other human rights. Additionally,

---

[6] For more information on trends: U.S. Federal Bureau of Investigation: Annual Reports of the Internet Crime Complaint Centre (IC3) retrieved from https://www.ic3.gov/media/annualreports.aspx or McGuire, M. and Dowling S., *Cyber Crime: A Review of the Evidence: Summary of Key Findings and Implications*, Home Office Research Report 75, U.K. Home Office, October 2013, p5. (https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence)

[7] Statistics Canada. Table 35-10-0001-01: Police-reported Cybercrime, by Cyber-related Violation, December 2018. Retrieved from https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=3510000101

[8] Canadian Centre for Justice Statistics: Policing Services Program, *Uniform Crime Reporting Incident-Based Survey: Reporting Manual*, March 2006, p. 52. Retrieved from: http://www23.statcan.gc.ca/imdb-bmdi/instrument/3302_Q7_V2-eng.pdf and Police-Reported Crime Statistics in Canada", *Juristat*, Canadian Centre for Justice Statistics, 2015, 2016 and 2017, Catalogue No.: 85-002-X, ISSN 1209-6393. Retrieved from: https://www150.statcan.gc.ca/n1/pub/85-002-x/2018001/article/54974-eng.pdf

the PCOCA introduced a new regime for rapidly preserving volatile data, using preservation demands and preservation orders.[9]

There is also a continued need for the IP21C Initiative in order to meet Canada's international obligations stemming from ratification of the Budapest Convention. Canada signed the *Council of Europe Convention on Cybercrime* (Budapest Convention) in November 2001 and ratified it on July 8, 2015. The reason it was not ratified sooner is that the Government needed time to bring into force domestic legislation to ensure Canada's laws complied with the convention – this was accomplished by PCOCA (former Bill C-13). The Budapest Convention is the main international instrument on cybercrime. It aims to help its state parties to harmonize their national laws, improve their investigative techniques, and increase international cooperation. Ratification of the Convention allows Canada to cooperate with other signatory countries in the investigation of cybercrime and enables access to digital evidence that may be found in another country. The number of parties to the Convention has grown over the years and currently stands at 64.[10] As noted later in section 4.2.4, Canada is viewed as playing a strong role in supporting the Convention internationally.

The evaluation evidence indicates that there is an ongoing need for the key activities funded by the IP21C Initiative, as summarized below:

- **Legal analysis, policy development and coordination on domestic and international issues –** While there has been very little litigation with respect to the IP21C investigative powers to date and no successful *Charter* challenges, Justice needs to maintain the capacity to defend any future challenges and to make future amendments to the *Criminal Code* as required. GAC also needs to continue to coordinate Canada's foreign policy approach on cybercrime in the international arena, which is becoming increasingly complex and politicised.

- **Awareness and training –** The "awareness" phase of the IP21C Initiative has ended, as prosecutors and law enforcement are now very familiar with the IP21C-related investigative powers. Outreach activities will continue to be needed to assist stakeholders in applying the *Criminal Code* provisions, primarily on a reactive or as needed basis. Ongoing training of prosecutors and law enforcement officials on the *Criminal Code* amendments has become integrated into the training programs offered by such organizations as the Canadian Police College and the PPSC School for Prosecutors. In addition, there has been ongoing training of foreign police and prosecution partners.[11]

- **Administration of data preservation scheme –** The IP21C Initiative has enabled the RCMP to develop and implement a data preservation scheme to handle a large volume of data preservation requests from foreign law enforcement. As Canada can reasonably expect to continue to receive preservation requests from foreign law enforcement, it must maintain a capability to manage such requests. The RCMP established a National Cyber Crime Coordination Unit to be a single point of contact.

- **Technical research and tools to support criminal investigations –** RCMP Technical Investigations Services have developed tools to access, obtain and process digital evidence from a device or digital storage medium seized as evidence (data at rest) as well as tools that are deployed in a live communications situation (data in motion). As cybercrimes are becoming

[9] Department of Justice Canada, Modernizing the Criminal Code: Backgrounder, 2013, retrieved from https://www.canada.ca/en/news/archive/2013/11/modernizing-criminal-code.html
[10] Council of Europe, *Chart of signatures and ratifications of Treaty 185: Convention on Cybercrime*, 2019, retrieved from: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures
[11] Annual IP21C Initiative Performance Information 2015-16 to 2017-18.

increasingly more technologically complex, it will be critical for the RCMP and other federal agencies to develop additional tools to support criminal investigations.

- **Provision of international cooperation in criminal matters –** The *Mutual Legal Assistance in Criminal Matters Act* (MLACMA) gives Canada the legal authority to obtain court orders on behalf of countries that are parties to mutual legal assistance agreements with Canada. MLA requests are coordinated by the IAG in Justice, which acts on behalf of the Minister of Justice as the Canadian Central Authority for both incoming and outgoing MLA requests. The number of MLA requests seeking digital evidence is growing (from 81 in 2015-16 to 448 in 2017-18). In addition to allowing Canada to better support its bilateral and multilateral MLA partners with additional evidence gathering powers, IP21C officials reported that resources provided by the Initiative also enabled Canada to play an important and growing role in supporting the Budapest Convention and in promoting the Convention to non-treaty countries. For example, a considerable amount of effort is being devoted to the drafting of a Second Additional Protocol to the Cybercrime Convention, which aims to provide police and prosecutors from member countries with additional tools to seek quicker access to digital evidence to assist in the investigation and prosecution of criminal activity. Canada also plays an important role in promoting the Convention to non-treaty countries. There are important foreign policy benefits for Canada in reinforcing the continued relevance of the Budapest Convention. For example, one of the Convention goals is to have similar legal frameworks and approaches in member countries. In so doing, it sets a basis for the safeguards and tools, as well as providing a forum to discuss issues and develop cooperative agreements - all of which facilitates law enforcement's ability to respond to the international/trans-border aspects of cybercrime.

4.1.2 Alignment with Government Priorities

The IP21C Initiative reflects a commitment made by the GOC in 2013 to introduce legislation that would give police and prosecutors new investigatory powers to obtain digital evidence. Since then, there has been continuing focus on cybercrime and more broadly cyber security. Although the PCOCA modernized the investigatory powers in the *Criminal Code*, technology is evolving at a rapid pace and is creating challenges for law enforcement in conducting investigations related to major crimes.

The GOC announced in the October 2013 *Speech from the Throne* that new legislation would be introduced to give police and prosecutors new tools to effectively address cyberbullying, as well as new investigatory powers to address Internet and digital evidence associated with computers, tablets and cell phones.[12] Since then, cybercrime has continued to be of significant interest, along with cyber security in a digital age more broadly; balancing the benefits of the digital economy with public safety.[13]

Most key informants agreed that the subsequent legislation, i.e., the PCOCA, addressed a significant need to modernize legislative tools to combat cybercrime and computer-assisted crime, and therefore is aligned with government priorities in this regard. The legislative amendments were written purposively to be technology neutral, i.e., the intent is that the investigatory powers will continue to be used by law enforcement to obtain digital evidence as computers and communications technologies evolve. For example, the dial-number recorder warrant was introduced to the *Criminal Code* (section 492.2) in 1993. It allowed police to install and monitor a number recorder, which provided information

[12] Parliament of Canada, *Speech from the Throne to open the Second Session Forty First Parliament of Canada*, 2013, retrieved from: https://lop.parl.ca/sites/ParlInfo/default/en_CA/Parliament/procedure/throneSpeech/speech412
[13] Parliament of Canada, *Budget 2018*, retrieved from https://www.budget.gc.ca/2018/docs/plan/toc-tdm-en.html; Public Safety Canada, *National Cyber Security Strategy*, 2018, retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx

identifying or recording a telephone number or the location of a telephone from which a call originated, was received or was intended to be received.[14] It did not, however, address transmissions between devices over the Internet (sometimes called "traffic data").The amendment of this provision via the PCOCA allowed for the modernization of the section, which now covers a broader range of communications; i.e. in addition to telephone calls, it now includes data relating to the routing of emails and text messaging for example, but explicitly excludes content.

Justice officials noted that a guiding principle in designing the new investigative powers was "privacy with precision." As outlined later in this chapter, there has been very little litigation with respect to these powers to date. The fact that there has not yet been a successful section 8 *Charter* challenge indicates that the investigative powers were well designed to ensure that privacy rights were protected. For example, the tracking warrant provisions (section 492.1) distinguish between tracking "things" (such as a vehicle) which requires a 'reasonable suspicion' standard[15] versus tracking individuals (usually by tracking a cell phone carried by an individual) which requires the higher standard of 'reasonable grounds to believe'.[16] Justice officials noted that Canada differs from other countries in that the investigative powers include several production orders; this was done intentionally so that each order would address a different problem.

Perceived gaps in legislation

The legislative amendments made to the *Criminal Code* by the PCOCA were viewed by most key informants as an important step in the battle against cybercrime and computer-assisted crime. However, many identified perceived gaps in the current legislation.

The main issue relates to the challenges faced by law enforcement in obtaining access to basic subscriber information[17] (BSI) held by TSPs. Many key informants mentioned the June 2014 Supreme Court decision *R. v. Spencer*, which concluded that BSI linked to specific Internet activity should not be obtained without authority through a reasonable law, such as a warrant, except in exigent circumstances. The decision ruled in a child pornography case that police had violated the suspect's reasonable expectation of online privacy when investigators requested the BSI linked to the IP address being used without first obtaining a court order for those records. The ruling decided that there was a reasonable expectation of privacy under the *Charter* in respect of BSI that allowed a link to be made between a person's identity and the activities of the person being conducted online that were revealing of intimate information. The request by police for the TSP to disclose the information was thus a constitutionally-protected search that, in the absence of a specific authority (such as a warrant), was not authorized by law and thus violated the *Charter*.[18] Before this ruling, police routinely requested and received BSI directly from TSPs. In the absence of any specific law designed for access to BSI,

---

[14] Anne Turner, "Wiretapping Smart Phones with Rotary-Dial Phones' Law: How Canada's Wiretap Law is in Desperate Need of Updating," 2017 CanLIIDocs384, p.277 retrieved from: https://commentary.canlii.org/w/canlii/2017CanLIIDocs384.pdf

[15] Canadian criminal law distinguishes between the thresholds of "reasonable suspicion" and "reasonable grounds to believe" required in order for police officers to lawfully arrest persons, conduct certain forms of searches and to obtain warrants. Each of the amendments made to the *Criminal Code* by the PCOCA is associated with one of these two thresholds. For further information, see: Library of Parliament, *Legislative Summary: Bill C-13: An Act to amend the Criminal Code, the Canada Evidence Act, the Competition Act and the Mutual Legal Assistance in Criminal Matters Act*, Publication No. 41-2-C13-E, revised 28 August 2014, retrieved from: https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/LegislativeSummaries/PDF/41-2/c13-e.pdf

[16] Ibid.

[17] Basic subscriber information consists of basic identifying information that corresponds to a customer's telecommunications subscription and can include name, home address, phone number, email address, and/or IP address. For further information, see: *National Security Green Paper, Background Document*, p. 57, retrieved from: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-en.pdf.

[18] CBC Investigates, "RCMP boss Bob Paulson says force needs warrantless access to ISP user data", November 16, 2016, retrieved from: https://www.cbc.ca/news/investigates/police-power-privacy-paulson-1.3851955

current practice for police is to apply for a court order, often using a general production order provision that can be used to obtain any type of information, when they want to request a user's BSI other than in exigent circumstances. Key informants representing law enforcement stated that obtaining a court order takes time and additional paperwork. Also, at the beginning of an investigation, they do not always have sufficient grounds to obtain a court order (the authority most often used is a general production order under section 487.014 of the *Criminal Code*).

The literature review revealed that this is contrary to the situation in many foreign jurisdictions where their laws specifically permit law enforcement and national security agencies to obtain BSI.[19] In many cases, this can occur without prior judicial authorization (often called administrative access). These foreign jurisdictions include the U.S., Australia, Germany, Sweden, Ireland, Denmark, Spain, Finland, the Netherlands and Norway.

A second issue identified by key informants is the lack of a specific provision in the law to address challenges arising from the absence of an interception capability, and challenges in relation to encryption. Some have suggested adding a specific provision to the *Criminal Code* requiring telecommunications service providers to assist with accessing information that has been encrypted. Some key informants suggest it would be useful to have a legal mechanism to provide "backdoor" access or to decrypt data. Sophisticated criminals tend to use communications technologies that encrypt data (e.g., messaging apps) which pose challenges for law enforcement and prosecutors in their ability to access this information. A federal prosecutor noted that the number of authorized wiretaps has declined dramatically over the past few years due to encryption, forcing police to revert to other means of uncovering information, i.e., using undercover officers and informants. Many other countries impose a general legal requirement for Communications Service Providers (CSPs) to have interception capabilities on their networks.[20]

These issues – access to BSI, capability for interception, and challenges from encryption – have been studied extensively by the GOC in recent years. In 2016, the GOC issued a National Security Green Paper[21] and carried out a Consultation on National Security to help inform future changes to national security tools.

The Green Paper put forth the idea of creating specific authority for police access to BSI. However, the subsequent National Security Consultations found that most online respondents along with many experts and organizations were reluctant to accept new powers and tools to enhance Canada's investigative capabilities in a digital world. Additionally, the majority (70%) of the general public that responded to the online consultation questionnaire considered BSI to be as private as the content of their communications; 48% said BSI "should only be provided in 'limited circumstance' and with judicial approval" – similar to what is currently required.[22]

The Green Paper also put forward the idea of creating authorities aimed at addressing the challenges in relation to encryption and requiring telecommunication and Internet service providers to have interception and data-retention capability in their networks. In some cases, CSPs may not be able to perform the interception in response to a court order because the technical capability to intercept communications has not been built into their infrastructure. The National Security Consultations found

---

[19] Government of Canada, *Our Security, Our Rights: National Security Green Paper, 2016, Background Document*, 2016, retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-en.pdf

[20] Ibid. p. 58.

[21] Government of Canada, *Our Security, Our Rights: National Security Green Paper, 2016,* retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016/ntnl-scrt-grn-ppr-2016-en.pdf

[22] Government of Canada, *National Security Consultations: What We Learned*, 2017, p. 13, retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-nsc-wwlr/index-en.aspx

that 78% of respondents to the online questionnaire opposed intercept capabilities in legislation.[23] Views were equally strong against giving investigators the ability to compel individuals or companies to assist with decryption. Many organizations opposed "back doors" for law enforcement because they would weaken network security and leave them vulnerable to attack.[24] Based on the data gathered for this evaluation, stakeholders representing prosecutors and law enforcement are in favour of such legislation.

In response to the National Security Consultations, in May 2017 the House of Commons Standing Committee on Public Safety and National Security recommended no changes be made to the lawful access regime for subscriber information and encrypted information but that this Standing Committee continue to study such rapidly evolving technological issues related to cybersecurity.[25]

4.2 Performance

4.2.1 Awareness and knowledge of the investigatory powers

There is a high level of awareness and knowledge of the IP21C investigatory powers among law enforcement, prosecutors and TSPs. IP21C officials carried out a wide range of activities to raise awareness and knowledge of the legislative amendments made to the *Criminal Code* and of Canada's obligations under the Budapest Convention, both in Canada and internationally.

Although it pre-dates the IP21C Initiative, all of the key informants representing police, law enforcement and TSPs who participated in the consultations leading up to the PCOCA (i.e. former Bill C-13 and its predecessors) stated that this involvement enabled them to become familiar with the legislative amendments made to the *Criminal Code*. Subsequently, they shared this knowledge with their internal and external networks.

IP21C officials carried out a wide range of activities to raise awareness and knowledge of the legislative amendments and of Canada's obligations under the Budapest Convention, both in Canada and internationally.[26] For example, Justice CLPS made over forty presentations to various stakeholder groups, held one-off meetings with stakeholders and responded to numerous inquiries from law enforcement and prosecutors seeking guidance on the new investigative powers. Approximately 1,500 individuals have benefited from these presentations and meetings.[27] The IAG in Justice has provided over fifty training sessions to Canadian and foreign police and prosecutors on the new available powers and the circumstances in which they can be engaged.[28] Additionally, the IAG holds annual learning days, which bring together domestic and foreign police and prosecutors. The PCOCA as well as general discussions on international cooperation in a digital world have been agenda items at these sessions given the prevalence of such MLA requests to and by Canada. The IAG has also created guides and primers to assist relevant partners in understanding the tools available to them in seeking digital evidence, both through the MLA process and other less formal means of international cooperation.[29] Officials from PPSC Headquarters provided training to prosecutors in the regions; these

[23] Ibid, p. 14.
[24] Ibid. p. 14.
[25] House of Commons Canada, *Report of the Standing Committee on Public Safety and National Security: Protecting Canadians and their Rights: A New Road Map for Canada's National Security*, May 2017, p. 43, retrieved from: https://www.ourcommons.ca/Content/Committee/421/SECU/Reports/RP8874869/securp09/securp09-e.pdf
[26] Annual IP21C Initiative performance reports, 2015-16 to 2017-18.
[27] Ibid.
[28] Ibid.
[29] The IAG MLA resource materials are available: https://www.canada.ca/en/services/policing/justice/extradition.html

regional prosecutors in turn provided training to provincial prosecutors, police and justices of the peace located in the regions.

Few key informants representing law enforcement and prosecutors outside of the federal government could comment on any specific awareness and training activities undertaken under the IP21C Initiative. This may be partly due to the fact that several years have passed since these activities were carried out following enactment of the PCOCA.

4.2.2 Management of issues and consistency of implementation and interpretation of investigatory powers

Relatively few legal and operational issues have arisen related to implementation of the new investigatory powers. There have been very few court cases to date related explicitly to these powers and no successful section 8 *Charter* challenges.

One outstanding legal issue is that the new transmission data recorder warrant provisions do not provide access to basic subscriber information. Federal partners are closely monitoring the evolving jurisprudence in this area.

Finally, the evaluation evidence indicates that the investigatory powers have largely been consistently implemented across Canada.

The IP21C Initiative was intended to manage any issues arising from the implementation of the new investigatory powers added to the *Criminal Code* to ensure that these powers would be consistently implemented and interpreted. This section outlines the main issues that have arisen and the extent to which they have been successfully managed under the IP21C Initiative.

Legal issues

Very few legal issues related to IP21C investigative powers have arisen to date. The resources provided to the federal partners by the IP21C Initiative have helped them to manage the legal issues associated with the implementation of the legislative amendments made to the *Criminal Code*. For example, Justice officials provided legal advice following the Supreme Court's decision in *R. v. Spencer* and with respect to several litigation files before the Supreme Court pertaining to search and seizure (section 8 of the *Charter*) [30] and to the extraterritorial reach of production orders[31].

Though they anticipated that there would be numerous section 8 *Charter* challenges, IP21C officials indicated that there has been very little litigation at any level related to the investigative powers specifically. Nor have any legal challenges arisen related to other Acts amended by the PCOCA, such as the MLACMA. Recently, there was a lower level court case in Ontario that challenged the "reasonable grounds to suspect" threshold associated with a transmission data recorder (TDR) warrant, but it was unsuccessful and has not been appealed to date[32].

The relative lack of legal challenges reflects the extent to which investigative powers were well designed and in such a way as to enhance *Charter* compliance and reduce the likelihood of successful *Charter* challenges. In addition, some of the more controversial provisions included in previous legislative attempts were not included in former Bill C-13 (e.g., former Bill C-30 in 2012 had included provisions that would have provided access to BSI under an administrative legal authority (not a court

[30] Examples of section 8 cases include: *R. v. Marakah*, *R. v. Jones*, *R v. Reeves* and *R. v. Mills*.
[31] Examples of cases include *BC Attorney General v. Brecknell* and Newfoundland (*Newfoundland Court of Appeal Re: section 487.02 of the Criminal Code*).
[32] Ontario Superior Court of Justice, *R. v. Otto*, 2019 ONSC 2473.

order) in designated circumstances and that would have enacted requirements to ensure an intercept capability in TSP networks).

The main outstanding legal issue raised by law enforcement and prosecutors is that the new TDR warrant provisions (section 492.2) in the *Criminal Code* do not provide law enforcement with access to BSI. Rather, general production order powers are now frequently being used for BSI, which can be cumbersome and pose challenges in meeting the standards required for such orders. As a workaround, law enforcement in some provinces are using assistance orders (section 487.02) to obtain customer name and address information. In January 2019, the Newfoundland and Labrador Court of Appeal adopted a broad and expansive interpretation of police powers in relation to electronic data with its decision in *Re: section 487.02 of the Criminal Code* (2019 NLCA 6).[33] Police in that case had sought a TDR warrant under section 492.2. This warrant only allows for the gathering of "transmission data". In this case it was used to determine which telephone numbers were communicating with a particular identified cell phone, which was associated with an investigation. In addition, they sought a section 487.02 assistance order requiring the TSPs to also provide the RCMP with the subscriber information associated with those other telephone numbers. The Court ruled that section 487.02 could be used to order the production of subscriber information. Justice and federal partners are closely monitoring the evolving jurisprudence with respect to the TDR warrant provisions and are keeping internal stakeholders apprised of the implications of the court decisions for investigations and prosecutions.

Operational issues

The overall view of key informants is that most of the operational issues associated with the implementation of the investigative powers have been resolved. IP21C officials worked with stakeholders to provide advice and support as required.

Most key informants stated that it took a considerable amount of time to work out how the investigative powers should be used in practice. A few interviewees representing law enforcement, prosecutors and the TSPs stated there was confusion about the use of production orders in the first couple of years following enactment of the PCOCA. For example, if law enforcement used a general production order to obtain customer name, address and account information, it was not clear whether they also had to obtain other orders related to the investigation, such as transmission and tracking data. While different judges tended to have different views on this question in the first few years, the courts have since ruled that multiple orders (e.g., tracking warrant, transmission data recorder warrant and assistance order) can be covered by a single "omnibus order" (a general production order under section 487.014).[34] Law enforcement and prosecutors view this as a positive aspect of the PCOCA.

All of the TSPs interviewed stated that they devoted effort to educating law enforcement on their proper usage. The major TSPs have in-house legal departments that advise operational staff when they have questions on the orders that have been served. They also noted that the courts have been helpful in providing guidance on the proper usage of the investigatory powers. For example, in January 2016 the Ontario Superior Court in its decision *R. v. Rogers Communications* provided some clarity for police and prosecutors about how they can obtain customer information from TSPs through "tower dumps", which are the production of all of the records of a cell phone tower at a particular time.[35]

The annual transparency report published by TELUS states that the company challenged or declined to provide information on only 5% of court orders received in 2017, because it believed the court order

---

[33] Canadian Technology Law Association (CAN-TECH Law), "Transmission Data and Subscriber Information," February 7, 2019, retrieved from: https://www.cantechlaw.ca/news/transmission-data-and-subscriber-information
[34] See for example Ontario Superior Court of Justice, *R. v. Otto*, 2019 ONSC 2473.
[35] For a summary of this case see: *E-Commerce Law Reports*, Volume 16, Issue 01, retrieved from: http://www.mcinnescooper.com/wp-content/uploads/2016/06/ECLR-Jan-Feb-2016-pg-15-16.pdf

was invalid or over-reaching. The report also states that law enforcement continued to take due care in preparing their requests.[36]

The RCMP noted that TSPs are experiencing challenges in executing preservation requests and demands/orders (e.g., complexity of the request, locating the required data, mitigating impacts to servers and its users). All of the TSPs interviewed stated they are concerned with the rising costs resulting from responding to the large volume of court orders. TSPs are not compensated by law enforcement for this work. A key informant representing one of the TSPs explained that the absence of a compensation policy stems from a 2008 Supreme Court case (*Tele-Mobile Co. v. Ontario*, 2008 SCC 12) where TELUS Mobility sought compensation for the costs of complying with third-party production orders under the *Criminal Code*.[37] The Supreme Court dismissed the case, basing its decision on the concept of civic responsibility. A key informant representing one of the TSPs argued strongly that Canada should have "fair compensation" legislation, whereby TSPs would be compensated for responding to court orders, which exists in other countries. This key informant stated that a joint industry-government working group is studying this issue.

Issues associated with the rapid evolution of computer and communications technologies

Many key informants noted that technology is evolving at a rapid pace and is creating challenges for law enforcement when investigating suspected criminals who have, or are planning to commit major crimes (terrorism, child exploitation, etc.). Examples are as follows:

- **Encryption** – While the *Criminal Code* may give law enforcement the power to, for example, seize the laptops and cellphones of suspected criminals or to intercept communications in real time, the data may be encrypted and thus unreadable. Suspected criminals in Canada may be communicating with collaborators in other countries via private messaging apps and online chat forums that are protected by encryption. As noted in section 4.1.2, law enforcement would like to see legislation introduced requiring TSPs to provide "backdoor" access or to decrypt data.

- **Dark web** – Criminal activity on the dark web is of major concern to law enforcement domestically and internationally. The anonymity of the dark web poses significant problems for investigators, as the identity and location of users are hidden. Europol Crime Centre (EC3), with support from the Federal Bureau of Investigation, the U.S. Drug Enforcement Agency and the Dutch National Police shut down AlphaBay and Hansa, which were large criminal markets on the dark web.[38] As explained further in section 4.2.4, Canada is viewed by international stakeholders as an important player in supporting the efforts of Europol to combat criminality on the dark web.

- **5G networks** – Key informants indicated that 5G networks will pose major challenges to law enforcement. Europol, in its annual organised crime threat assessment,[39] highlighted that this new communications technology will threaten existing techniques for tracking criminals. The agency has stated that the tools and techniques to carry out surveillance on 4G networks are "one of the most important investigative tools that police officers and services have" and that

---

[36] TELUS, "Transparency Reporting", retrieved from: https://www.telus.com/en/about/sustainability/sharing-our-progress/transparency-reporting
[37] For further information on this case, see: *Law Times*, "2nd Opinion: Civic responsibility on the wane", retrieved from: https://www.lawtimesnews.com/article/2nd-opinion-civic-responsibility-on-the-wane-9682/
[38] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018*, retrieved from: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018
[39] Ibid.

police forces may not be able to track criminals effectively over 5G networks.[40] Europol stated that discussions were underway with technology firms and governments on how to close the surveillance gap.

Cross-border jurisdictional issues

IP21C officials are devoting considerable effort, as evidenced in performance reports, to dealing with cross-border jurisdictional issues associated with the investigation and prosecution of transnational cybercrime and computer assisted crime.[41] An example is where the crime may have taken place in Canada but digital evidence is stored in the cloud or on servers located outside Canada (e.g., Facebook has data centres in the U.S. and in several other countries).

Law enforcement in Canada and elsewhere face challenges in serving production orders on companies located in other countries. The MLA process is viewed by some domestic and foreign partners as taking too long and therefore law enforcement and prosecutors look for other ways of obtaining information. Canadian law enforcement and prosecutors would like to have the ability to directly access data that was generated in Canada but stored on foreign servers; however, this approach can have significant sovereignty and jurisdictional implications, and can impair Canada's relationships with its foreign partners in the area of MLA if foreign law and procedure are not respected in seeking direct cooperation.

The Budapest Convention contains provisions on MLA, but the process is considered to be inefficient at times, given the legal and procedural protections in place to protect privacy and other human rights. These protections have in some cases led to delays in providing MLA quickly, particularly with respect to obtaining electronic evidence. The Parties to the Convention have been looking for ways to streamline the MLA process. A major effort is being devoted to drafting of the Second Additional Protocol, which is intended to address challenges to obtaining digital evidence for criminal justice purposes more efficiently. This new protocol is discussed further in section 4.2.4.

The U.S. passed the CLOUD Act in March 2018, which allows federal law enforcement to compel U.S.-based technology companies via warrant or subpoena to provide requested data stored on servers regardless of whether the data is stored in the U.S. or on foreign soil. It also provides an alternative to the MLA process through reciprocal "executive agreements", whereby foreign countries that enter into such agreements with the U.S. can directly serve legal process requests on U.S. providers for access to their data, and the U.S. can do the same in return. This is a promising development that may result in addressing on a bilateral basis some significant challenges and contains a number of significant human rights safeguards. A review of the literature indicates that while it is supported by the US government, the UK government, the Australian government, the European Union as well as by major US companies, the Act is not without controversy. Many civil liberties groups, such as the American Civil Liberties Union, have criticized the Act. For example, one criticism is that it does not contain any prompt mechanism for withdrawal from the executive agreements once they have been made, even if one of the participants suddenly starts to abuse civil liberties.[42] The U.S. and the UK recently completed negotiations and have produced a final agreement, which is the first executive agreement under the CLOUD Act. IP21C officials stated that Canada will continue to monitor developments in this area with interest, as executive agreements would appear to have the potential to assist with some pressing problems in addressing serious crimes arising from evolving technology and related cross-border investigative challenges. The Canadian Association of Chiefs of Police and the International Association of Chiefs of Police have both called on the federal government to pursue

---

[40] BBC News, "Police will struggle to track criminals via 5G", July 19, 2019, retrieved from: https://www.bbc.com/news/technology-49043822

[41] Annual IP21C Initiative performance reports, 2015-16 to 2017-18.

[42] *Canadian Lawyer*, "Dark Cloud", April 16, 2018, retrieved from: https://www.canadianlawyermag.com/author/lisa-r-lifshitz/dark-cloud-15600/

discussions with the US on this subject given the potential to create a useful mechanism for law enforcement.[43]

Consistency of implementation and interpretation of investigatory powers

The degree of consistency in the implementation and interpretation of the investigatory powers was examined by determining whether there have been any legal challenges to the *Criminal Code* provisions. Following enactment of the PCOCA, Justice CLPS worked to support consistent implementation by making over forty presentations at conferences of investigators and to national committees involving police at the national, provincial and municipal levels.[44] Legal advice was provided to federal partners on the new provisions to support international work, such as the efforts by Canada to support the drafting of the Second Additional Protocol.

While the evaluation evidence indicates that the IP21C Initiative has helped to ensure that the investigatory powers have largely been implemented in a consistent fashion, key informants noted that there is an inconsistency in whether courts will grant police a production order requiring a non-Canadian company to produce digital evidence. The literature review found that court decisions have varied in terms of whether production orders could be obtained against foreign companies that host Canadians' data on servers outside Canada. Some courts have refused to grant an order where the company is wholly outside of Canada, while others have granted such orders on the basis that a foreign company that contracts with users in Canada and hosts their data is subject to the jurisdiction of Canadian courts.[45] A January 2018 B.C. Court of Appeal decision – *British Columbia (Attorney General) v. Brecknell* – has implications for foreign companies with a "virtual presence" in Canada. [46] In 2016, the RCMP applied to the B.C. Provincial Court for a production order requiring Craigslist to produce certain information about one of its users, consisting of the user's name, address, IP address, phone number and all relevant information associated with a post. The court refused on the basis that Craigslist had only a virtual presence in B.C. The RCMP appealed, and the B.C. Court of Appeal agreed: Craigslist is "present in the province of B.C. and police can obtain a production order naming it, even though it has no physical presence in Canada or an address in Canada to effect."

Some legal commentators were surprised by the *Brecknell* decision, stating that the Court's decision appears to give extra-territorial effect to production orders – which they argue was not the intent of Parliament in drafting the legislation.[47] There is also the question of whether, from a practical standpoint, such orders can be enforced outside Canada.

In a more recent case that was being litigated in Ontario (now concluded), the London Police Service obtained a Canadian production order to compel Facebook to produce data for a murder prosecution pending before the Superior Court of Ontario. Facebook voluntarily produced subscriber data but directed the Canadian police to make an MLA request to the U.S. for the content data sought, so that the U.S. could pursue a U.S. order to compel production. The Canadian authorities continued to pursue the production order with Facebook, leading the latter to apply to the Canadian court to have

---

[43] Canadian Association of Chiefs of Police, CACP Resolution Status Report, June 2017, p.9, retrieved from https://www.cacp.ca/status-report-government-responses.html?asst_id=1433

[44] Annual IP21C performance reports, 2015-16 to 2017-18

[45] For a discussion of this issue see: Christopher P. Naudie and John Cotter, "Canada: Cross-Border Investigations: B.C. Court Affirms Broad Power to Issue Legal Process Against Foreign Companies", retrieved from https://legalyearinreview.ca/cross-border-investigations-b-c-court-affirms-broad-power-issue-legal-process-foreign-companies/?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original

[46] For an analysis of the *Brecknell* decision, see David Fraser, "The Legal Reality: Canadian Appeal Court decides "Virtual Presence" is enough for production order for user information against non-Canadian company", *CanLII Connects*, retrieved from: https://canliiconnects.org/en/commentaries/54673

[47] See for example Osler, "Cross-border investigations: B.C. Court affirms broad power to issue legal process against foreign companies, retrieved from: https://legalyearinreview.ca/cross-border-investigations-b-c-court-affirms-broad-power-issue-legal-process-foreign-companies/#_ftn7

the order set aside on the basis that it had no force of law in the U.S. An MLA request for the data was ultimately made and executed. Facebook subsequently withdrew its application on the basis of mootness, bringing the matter to an end.[48]

4.2.3 Improved operational ability to combat cybercrime & computer-assisted crime

The IP21C Initiative has contributed to improving Canada's operational ability to combat cybercrime and other computer-assisted crimes. IP21C officials have collaborated extensively with each other and with external stakeholders to support implementation of the IP21C-related investigatory powers. The RCMP has implemented a dedicated triage function to manage data preservation requests received from foreign law enforcement. The RCMP also has developed new tools to access, obtain and process digital evidence from devices seized as evidence as well as tools used in a live intercept situation.

Formation of partnerships and increased cooperation and collaboration

IP21C officials reported extensive collaboration with each other and with external organizations and groups to support the implementation of the IP21C Initiative. For example, Justice CLPS has developed a close working relationship with police by participating in such fora as the annual meeting of child exploitation investigators and the Counter-Terrorism and National Security Forum. Following enactment of the PCOCA, numerous meetings were held with the telecommunications industry and with federal and provincial law enforcement officials. Justice IAG has formed close working relationships with law enforcement and prosecutors across Canada and also does outreach to internet service providers (ISP) whose data is frequently sought by foreign partners to advance their criminal investigations and prosecutions. For example, 43% of incoming MLA requests in 2017-18 sought digital evidence.

Implementation of a dedicated triage function for international requests for data preservation

The RCMP has developed and implemented a dedicated triage function to administer a new data preservation scheme that is in accordance with the legal provisions in the PCOCA and to respond to international requests to preserve digital evidence under the *Criminal Code*, in anticipation of the foreign state seeking MLA from Canada to obtain the preserved evidence. This has involved such activities as staffing the function, developing standard operating procedures, and designing a tracking system.

The RCMP receives data preservation requests from foreign law enforcement (as do other police forces across Canada). Data preservation requests pertaining to child exploitation investigations are received by RCMP Technical Operations (National Child Exploitation Crime Centre) while all other requests are handled by Federal Policing. In most cases, the RCMP will serve a preservation request to the Canadian TSP. The TSP then advises the RCMP of its standard data retention period according to the company's data retention policy. In cases where data will not be saved long enough for the MLA process to be completed, the RCMP will serve a preservation demand, which is valid for 90 days. In cases where the MLA process is not completed within the 90-day window, just prior to the expiry date the RCMP will serve the TSP with a preservation order, which extends the window for another 90 days.

[48] CBC news, "London, Ont., court to decide if police can access Facebook messages", retrieved from: https://www.cbc.ca/news/canada/london/london-ontario-facebook-messages-legal-case-homicide-investigation-1.5149023

The review of RCMP performance reports revealed that a total of 176 data preservation requests were received in 2016, which increased substantially to 505 in 2017. Of this total, 408 requests were received by Federal Policing, of which 286 (70%) were for preservation requests (the initial step in the process as noted above), 117 (29%) were for preservation demands and 5 (1%) were for preservation orders. In 2018, the number of data preservation requests received by Federal Policing declined substantially. A Canadian ISP that had been served the largest number of requests opened a sub-office in the US. As a result, US authorities began to interact with this sub-office rather than make requests to Canada.

Improved processing of mutual legal assistance requests

Funding provided by the IP21C Initiative has enabled Justice IAG to increase its capability to process both incoming and outgoing MLA requests. The level of collaboration with the RCMP has also increased. This topic is discussed in detail in section 4.2.4.

Development of new technical tools

The IP21C Initiative has provided funding to the RCMP that contributed to the development of new tools to access, obtain and process digital evidence from devices and digital storage media (data at rest) as well as tools used for warranted, real-time interception of transmission data (data in motion).

Usage of the IP21C-related investigatory powers

Most key informants, including IP21C officials and representatives from law enforcement, prosecutors and TSPs, confirmed that the investigatory powers added to the *Criminal Code* are being used. Key informants representing law enforcement and prosecutors generally agreed that these powers are now well integrated into the investigator's "toolbox". TSP representatives stated that most of the court orders served by law enforcement on Canadian TSPs relate to production orders (ss. 487.014 to 487.018). Preservation demands and orders account for a smaller proportion of the total, which corresponds to the RCMP performance data. A key informant representing law enforcement noted that the production order for trace communications (section 487.015) is rarely used. This order is intended to be used to trace rerouted communications through multiple TSPs, even though the identity of one or more of the providers is not known at the time the order is sought.

Two of the major TSPs, TELUS and Rogers, publish annual transparency reports in accordance with the Voluntary Transparency Reporting Guidelines issued by Innovation, Science and Economic Development Canada in 2015. These reports provide some high-level information on usage of the investigatory powers. (Key informants representing the TSPs noted that caution should be taken when interpreting this data, as the companies count court orders in different ways.) The TELUS report shows that the number of court orders increased from 3,550 in 2014 to 4,871 in 2018.[49] No breakdown is provided by the various *Criminal Code* provisions. The 2017 Rogers report shows that the number of court orders declined from 115,954 in 2016 to 100,708 in 2017 (no explanation is provided on the reason for the drop). The number of tower dump production orders increased from 191 in 2016 to 511 in 2017.[50] Key informants representing the major TSPs noted that law enforcement is making increasing use of tower dumps.

[49] TELUS, op. cit.
[50] Rogers Communications, "2017 Rogers Transparency Report", retrieved from: https://about.rogers.com/2018/05/17/2017-rogers-transparency-report/

4.2.4 Improved international cooperation to obtain digital evidence

The IP21C Initiative has helped Canada to increase its level of cooperation internationally to obtain digital evidence to combat cybercrime and computer-assisted crime. Canada is viewed by international stakeholders as being in compliance with the requirements of the Budapest Convention. The Initiative has also contributed to improved coordination and consistency in Canada's foreign policy approach on cybercrime and computer-assisted crime.

Ratification of the Budapest Convention

As noted earlier, Canada signed the *Council of Europe Convention on Cybercrime* (Budapest Convention) in November 2001 and ratified it on July 8, 2015. The reason it was not ratified sooner is that the Government needed time to bring into force domestic legislation to ensure Canada's laws complied with the Convention – this was accomplished by PCOCA (former Bill C-13). Canada is viewed by international stakeholders as being in compliance with the requirements of the Budapest Convention.

Second Additional Protocol

The Budapest Convention contains MLA provisions, but the process is considered overburdened by the increasing volume of requests for digital evidence. Some perceive the process as being too slow to effectively access data in the modern context. The Parties to the Convention have been looking for ways to streamline the process, while preserving the safeguards necessary to accessing such data. They considered regulating trans-border access to stored data by extending the interpretation of Article 32 of the Convention; however, this attempt ended inconclusively in 2014. The Cybercrime Convention Committee (Council of Europe) (T-CY) Cloud Evidence Group (CEG) was established in December 2014 to explore solutions for access to evidence in the cloud for criminal justice purposes, including through MLA. The CEG produced a report in September 2016; the main recommendation to T-CY was to consider preparation of a draft Protocol to the Budapest Convention. The Terms of Reference for the Preparation of a Draft Second Additional Protocol were approved by the T-CY on June 8, 2017. [51] The scope includes: provisions for more effective MLA (a simplified regime for MLA requests for subscriber information; international production orders; direct cooperation between judicial authorities in MLA requests); and provisions allowing for direct cooperation with service providers in other jurisdictions with regard to requests for subscriber information, preservation requests and emergency requests.

Canada is playing a major role in the drafting of the Second Additional Protocol. There are two plenary sessions and four to six expert drafting sessions annually. There have been ten concept papers which clarify specific problems and, when appropriate, suggest possible treaty provisions. Canada has led the preparation of two of the concept papers.[52]

Processing of mutual legal assistance requests

The *Mutual Legal Assistance in Criminal Matters Act* (MLACMA) gives Canada the legal authority to obtain court orders on behalf of countries that are parties to MLA agreements with Canada. These include bilateral treaties and multilateral conventions containing provisions for MLA. Canada is also

[51] NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE), "Council of Europe Ponders a New Treaty on Cloud Evidence", retrieved from: https://ccdcoe.org/incyder-articles/council-of-europe-ponders-a-new-treaty-on-cloud-evidence/

[52] The draft version of this and other provisions related to the Second Additional Protocol are available on the Council of Europe website at: https://www.coe.int/en/web/cybercrime/t-cy-drafting-group

able to enter into case-specific and time-limited administrative arrangements under the MLACMA, in appropriate cases, to assist a non-treaty country to obtain MLA including digital evidence from Canada. The PCOCA made significant changes to the MLACMA by incorporating many of the new investigative powers that were added to the *Criminal Code*, thereby allowing Canada to provide evidence to foreign partners under those provisions in appropriate circumstances. IAG officials noted that the PCOCA and the associated amendments made to the MLACMA provided several benefits for the MLA process. The main changes were to the provisions regarding tracking and transmission warrants as well as production orders (evidence gathering orders) and the inclusion of preservation demands and orders in the *Criminal Code*, which can be sought by domestic and foreign law enforcement authorities. The new provisions give the MLA judge who issues the order/warrant, the discretion to dispense with a separate hearing called the "sending hearing" which is generally a procedural requirement under the MLA process. This streamlined the process, which is important given records obtained by tracking or transmission data recorder warrants or pursuant to one of the new production order powers, are often time sensitive. In sum, the PCOCA amended the *Criminal Code* and the MLACMA so that the production orders and preservation demands and orders added to the *Criminal Code* became available to assist foreign investigations.

Canada has signed bilateral MLA treaties with 35 countries and has also ratified several international conventions containing provisions on MLA, such as the *United Nations Convention against Transnational Organized Crime* and the *United Nations Convention Against Corruption*.[53] Canada's ratification of the Council of Europe *Convention on Cybercrime* gained numerous new MLA partners, and the number continues to grow.

Justice IAG coordinates all MLA requests made by Canada as well as those made to Canada. To process MLA requests, the IAG deals with Canadian and foreign law enforcement agencies and prosecutors, as well as with the central authorities of other countries. The IAG reviews the requests and ensures that the supporting documents and evidence are sufficient to meet the treaty requirements and those of Canadian law, and that required authorizations have been issued. The volume of MLA requests was expected to increase as a result of the PCOCA and ratification of the Budapest Convention. The IAG maintains statistics on the number of MLA requests coming into Canada (incoming) and made by Canada to other countries (outgoing). Of the total of approximately 1,050 active incoming MLA requests in 2017-18, 43% (448 requests) sought digital evidence. The total number of MLA requests has increased substantially over the years.

Statistics on the volume of MLA requests seeking digital evidence processed by Justice IAG during the time period covered by the evaluation are presented in Table 3.

Table 3: Number of incoming and outgoing MLA requests seeking digital evidence

Year	Number of Incoming MLA Requests Seeking Digital Evidence Received by IAG			Number of Outgoing MLA Requests Seeking Digital Evidence Made by IAG		
	Under the Budapest Convention	Under Other Treaties & Admin. Arrangements	Total	Under the Budapest Convention	Under Other Treaties & Admin. Arrangements	Total
2015-16	0	405	405	0	97	97
2016-17	10	354	364	0	128	128

[53] Global Affairs Canada maintains a list of bilateral and multilateral treaties at: https://treaty-accord.gc.ca/section.aspx?lang=eng

Year	Number of Incoming MLA Requests Seeking Digital Evidence Received by IAG			Number of Outgoing MLA Requests Seeking Digital Evidence Made by IAG		
	Under the Budapest Convention	Under Other Treaties & Admin. Arrangements	Total	Under the Budapest Convention	Under Other Treaties & Admin. Arrangements	Total
2017-18	14	434	448	1	113	114

The total number of incoming MLA requests seeking digital evidence fluctuated over the three-year period, reaching a high of 448 requests in 2017-18. The volume of outgoing requests is much lower and also fluctuated over the three years. Several representatives of Canadian law enforcement stated that they will avoid the lengthy MLA process if at all possible. While there is a perception that the MLA process is relatively slow in many countries, the Council of Europe does not compile statistics on the amount of time taken by Member Parties to process MLA requests.

Relatively few requests are received under the Budapest Convention, as parties make use of existing treaties and other conventions first. As noted above, Canada has bilateral agreements with many countries and has ratified several multilateral conventions.

IAG statistics show that just over four months are required to execute incoming MLA requests.[54] IAG officials noted that many of the simple requests from countries with similar legal systems are executed in a shorter period of time. The nature of incoming MLA requests is becoming increasingly complex. Requests from countries with similar systems, such as the U.S., are generally more straightforward; one-off requests from other countries can take more time, as the country may not be familiar with Canada's legal and procedural requirements, and will require guidance on seeking cooperation from Canada. In addition, there may be translation issues, amongst others. Canada also experiences delays in obtaining digital evidence from other countries.

Funding provided by the IP21C Initiative has helped the IAG to improve the management of MLA requests. IAG has created and staffed an MLA Cyber Unit. Multiple training tools have been developed, including a step-by-step MLA Guide posted on the IAG's public website and primers on the PCOCA as it relates to the MLA process and how to seek compelled data preservation. Draft requests are shared with the Canadian competent authority at an early stage, so that any gaps or issues requiring clarification can be sent to the foreign central authority. The extensive outreach carried out by IAG has also helped improve the overall functioning of the MLA process.

Finally, Canada is viewed as being in compliance with the MLA provisions of the Budapest Convention. The Council of Europe (its T-CY Committee) has done three rounds of assessments of each party's level of compliance. The 2017 assessment report[55] notes that Canada has implemented several best practices, such as establishing a 24/7 point of contact for MLA requests; maintaining a database of MLA requests; establishing a cyber-unit within the Central Authority (JUS-IAG); accepting requests electronically; and, maintaining a comprehensive public website providing substantive guidance to foreign authorities on making effective MLA requests. International key informants stated that other countries can benefit from Canada's experience.

[54] This figure is for requests that are complete; additional time may be devoted to back-and-forth communications with the requesting central authority to obtain missing information and clarify any issues.
[55] Council of Europe, "Assessing the implementation of the Budapest Convention", retrieved from: https://www.coe.int/en/web/cybercrime/assessments

Canada's foreign policy approach to cybercrime

The resources provided to GAC (a total of two FTEs) by the IP21C Initiative have enabled officials to focus on the work required to help ensure Canada has an integrated and consistent foreign policy approach to cybercrime. GAC has consulted and coordinated inter-departmentally to support the foreign policy work. GAC officials coordinate Canada's active participation in international initiatives to combat cybercrime. This work takes place in several fora, including the G7, the United Nations Office on Drugs and Crime, the Organization of American States (OAS), and the Council of Europe.

As noted above, Canada is playing a prominent role in supporting the Budapest Convention. International key informants noted that Canada's contribution has grown substantially over the past few years. Contributing to the operation of the Convention requires a considerable effort. Federal officials attend the twice-yearly meetings of the Cybercrime Convention Committee (T-CY), participate in the four to six protocol drafting sessions, as well as the periodic "Octopus" conference.[56] A Justice official was elected to the T-CY Bureau in 2016 and was nominated for a second term in 2018. Canada also plays an active role in promoting the Convention to countries that have not yet ratified it.

Although it is not directly related to the IP21C Initiative, Canada is viewed as being highly committed to the work of Europol's European Crime Centre (EC3). Europol set up EC3 in 2013 to strengthen the law enforcement response to cybercrime in the European Union (EU) and thus help to protect European citizens, businesses and governments from online crime. Canada via the RCMP is a member of J-CAT (Joint Cybercrime Taskforce) which works on the most important cybercrime cases that affect EU Member States. An RCMP liaison officer is stationed at EC-3 in The Hague, Netherlands, and Canada is adding a second staff member in 2019-20. Canada is considered to be a leader in combating online child sexual exploitation. It is also a full player in EC3's "Dark Web Team".

Support for capacity-building

The IP21C Initiative provides a small amount of funding ($250K annually) to augment the funding provided to a project under GAC's Anti-Crime Capacity Building Program. This project, led by the OAS, provides support to the Inter-American Committee Against Terrorism to provide technical training to cyber security stakeholders in 26 Member States in Latin America and the Caribbean.

4.2.5 Unintended Impacts

Key informants representing the TSPs noted that responding to court orders has a real impact on costs and believe that this impact was not considered in the drafting of the legislative amendments. As noted earlier, the TSPs are calling on the GOC to introduce legislation whereby they would be compensated for the costs incurred.

The main unintended impacts identified by key informants pertain to the aftermath of the *Spencer* decision in 2014 and are not related specifically to implementation of the IP21C-related investigatory powers. However, they have affected how these powers are being used. For example, TSPs no longer provide subscriber information to law enforcement on a voluntary basis (except in exigent circumstances) and instead require a general production order. Consequently, the number of production orders served to TSPs is likely much greater than anticipated when the legislative amendments were being designed.

[56] The Octopus Conference is held every 12 to 18 months by the Council of Europe and each conference focusses on a specific cybercrime issue. Retrieved from https://www.coe.int/en/web/cybercrime/octopus-conference.

4.3 Design

4.3.1 Horizontal management of the IP21C Initiative

The IP21C Initiative has been well coordinated. The IP21C Initiative business plan was thoroughly prepared and the Initiative has evolved as expected.

The IP21C officials interviewed indicated that the Initiative has been well coordinated. They stated that the IP21C Initiative business case was thoroughly prepared. It is clear from the findings presented in this chapter that the Initiative has evolved as anticipated.

One of the federal partners indicated that it would like to have more information on the work carried out by other IP21C officials in supporting the Initiative. A question was raised as to whether an inter-departmental working group focussing on cybercrime should be established, but it was noted that a new interdepartmental committee had recently been formed that should address this need.

A performance measurement strategy was developed at the outset of the Initiative to support the evaluation. Although a few IP21C officials noted challenges collecting the data due to limitations extracting the information from records management systems, they were able to provide the required information on an annual basis.

5. CONCLUSIONS AND RECOMMENDATIONS

5.1 Conclusions

The conclusions of the horizontal evaluation of the IP21C Initiative with respect to the evaluation issues are summarized below.

5.1.1 Relevance

The overall objective of the IP21C Initiative – to provide the means to implement the amendments made to the *Criminal Code* and the other acts by the PCOCA and to meet Canada's international obligations stemming from ratification of the Budapest Convention – continues to be relevant, as cybercrime is growing at a fast rate both in Canada and internationally, and criminals are increasingly exploiting evolving technologies. The main activities supported by the IP21C Initiative should continue.

While the evaluation evidence indicates that the PCOCA responded to a commitment made by the GOC in 2013 to modernize the investigatory powers in the *Criminal Code*, Canada's laws need to continually evolve so that law enforcement and prosecutors are equipped with the tools necessary to combat major crimes. Police and prosecutors highlighted in particular the challenges associated with obtaining access to BSI and encrypted data.

5.1.2 Performance

The target audiences of the IP21C Initiative, including law enforcement, prosecutors and telecommunications service providers are now very familiar with the legislative amendments made to the *Criminal Code* and other acts. IP21C officials devoted considerable effort to raising awareness and knowledge of the key elements of the PCOCA.

Relatively few legal and operational issues have arisen related to the new investigatory powers. While it was expected that numerous *Charter* challenges would arise from the new investigative powers, this has not yet proved to be the case. The resources provided to the federal partners by the IP21C

Initiative have helped them to manage implementation of the investigatory powers in a variety of ways, ranging from supporting prosecutions that rely on these powers to providing internal and external stakeholders with legal and policy advice. The main legal issue raised by key informants is that the new transmission data recorder warrant provisions do not provide access to basic subscriber information. The investigatory powers have largely been consistently implemented across Canada.

The IP21C Initiative has contributed to improving Canada's operational ability to combat cybercrime and other computer-assisted crimes. IP21C officials have collaborated extensively with each other and with external stakeholders to support implementation of the IP21C-related investigatory powers. The RCMP has implemented a dedicated triage function to process and track data preservation requests received from foreign law enforcement. It also has developed new tools to access, obtain and process digital evidence from devices seized as evidence, as well as tools used in a live intercept situation.

The IP21C Initiative has helped Canada to increase its level of cooperation internationally to obtain digital evidence to combat cybercrime and computer-assisted crime. Canada is viewed by international stakeholders as being in compliance with its requirements. Canada is viewed internationally as playing an important role in supporting the Budapest Convention, with considerable effort devoted to the drafting of the Second Additional Protocol. Justice IAG has improved the processing of MLA requests seeking digital evidence received from foreign law enforcement. The Initiative also contributed to improved coordination and consistency in Canada's foreign policy approach on cybercrime and computer-assisted crime.

5.1.3 Design

The IP21C Initiative has been well coordinated. The IP21C business plan was thoroughly prepared and the Initiative has evolved as expected.

5.2 Recommendations

As noted, the IP21C Initiative stems from the portions of the LAI relating to the amendments to the *Criminal Code* and the other Acts by the PCOCA and to meet the international obligations stemming from ratification of the Budapest Convention. Consequently, the IP21C partners were already engaged in the broader operational areas within which the IP21C-specific activities are situated.

No recommendations are included as the Initiative has been implemented as expected, and there are no identified barriers to the achievement of expected results. While several issues were raised, such as access to BSI and encrypted data, they are beyond the scope of the Initiative or are matters before the courts.

APPENDIX A: PROGRAM PROFILE

A.1 Governance

The IP21C Initiative is overseen by senior officials from each partner department or agency who are jointly responsible for managing its implementation, while each executes its specific activities in the criminal justice and international policy systems. Justice is responsible for leading the coordination of policy and legal advice to ensure the consistency, while respecting the independence of federal organizations within their own mandates.

A.2 Linkages

IP21C Initiative is linked with the GOC's Cyber Security Strategy that is focussed on making cyberspace more secure for all Canadians, and to the LAI, which is focussed on ensuring that criminal and national security threats are identified and acted upon while respecting the privacy of Canadians.

A.3 Roles and Responsibilities of IP21C Partners

i) Department of Justice Canada

The Department of Justice supports the amendments enacted in the PCOCA and ensures that the provisions concerning the investigative powers associated with digital evidence are successfully integrated into the Canadian justice system. This includes developing and providing training to the law enforcement community, prosecutors and service providers; providing legal and policy advice to support implementation; and providing expertise on any *Charter* related issues.

The Criminal Law Policy Section provides legal and policy advice to support implementation of the new investigative powers. It was involved in the development and delivery of awareness and training activities to ensure that the PCOCA amendments were understood, interpreted and implemented consistently to minimize risk of misinterpretation or misapplication.

The Human Rights Law Section provides expertise related to the *Charter* as well as related litigation support.

The International Assistance Group is responsible for the review and execution of all requests made to and by Canada seeking MLA in criminal matters and extradition.

The RCMP Legal Services Unit (LSU) provides legal advice and support to the RCMP on legal and policy issues arising from the implementation and application of the IP21C provisions.

ii) Public Prosecution Service of Canada

The PPSC is responsible for responding to investigator requests for legal advice and support in the context of investigations and prosecutions as a result of amendments to sections 492.1 and 492.2 of the *Criminal Code* and the creation of new production and preservation orders (especially in high complexity cases and in a major proportion of medium complexity cases).[57] The PPSC Is also involved at the pre-charge stage. Moreover, the PPSC is increasingly involved at the post-charge stage due to lengthier prosecutions, resulting when there are constitutional challenges to the new legislation, and

[57] Other amendments that resulted in increased PPSC involvement at the pre-charge stage included the new omnibus order provisions in 184.2(5), 186(8) and 188(6), specifically the words "related to the execution of the authorization" and the new sealing order provision in 187(7).

the development of new precedents. The PPSC also provides training to prosecutors and some police officers. Training occurs at the annual PPSC School for Prosecutors and in regional offices on a periodic basis. Ongoing workshops and updates to training materials for prosecutors and/or police occurred as the new provisions were implemented and interpreted by the courts.

iii) Royal Canadian Mounted Police

The RCMP has a broad mandate in addressing cybercrime, both domestically and internationally. This includes addressing crimes where the Internet and information technologies are used in the commission of a criminal offence. Under the IP21C Initiative the RCMP is responsible for the following initiatives:

- The development of a dedicated triage function to administer a new data preservation scheme, and to respond to foreign country requests for assistance related to IP21C, including the Budapest Convention. Part of this function is embedded with the RCMP's National Child Exploitation Crime Centre as well as linked with key Federal Policing operational areas for requests that fall outside of those related to child exploitation. The RCMP's National Operations Centre serves as the "24/7" point of contact to facilitate the provision of technical advice and legal information, preservation of data, collection of evidence and locating suspects in relation to international requests under the Budapest Convention.

- The development of new technical tools and/or solutions for warranted, real time interception of transmission data and analysis of seized data. This includes network interception tools, alternative data capture tools, processing tools, and the formatting of data for investigative, analytical and evidentiary purposes. New operational tools have been developed to collect data from tracking devices in real time to locate a person, transaction or thing. The tools support domestic and international investigations involving Canada's major telecommunications services. Research and development activity is embedded in RCMP Special "I" programs and Integrated Technological Crime Units (ITCUs) located in Ontario, Quebec and British Columbia.

- New dedicated resources to augment criminal investigative teams and implement tools for the real time interception of transmission data and analysis of seized data related to the IP21C investigative powers, including international requests related to the Budapest Convention. This element focusses on the operational implementation and use of the new tools in criminal investigations. Resources are housed in the RCMP Special "I" programs and ITCUs located in Ontario, Quebec and British Columbia.

The RCMP's roles and responsibilities with respect to IP21C Initiative are supported by the RCMP LSU. There has been ongoing engagement with the RCMP LSU to support RCMP training on the new investigative powers under the PCOCA, the new obligations of the RCMP arising from the ratification on the Budapest Convention, and on legal developments in this area of law affecting RCMP operations. Training also included in-house training activities with RCMP operational areas, with the engagement of the RCMP Legal Application Support Teams.[58]

iv) Global Affairs Canada

GAC supports implementation of the PCOCA and the Budapest Convention by advancing international cooperation on cybercrime and ensuring that Canada's interests related to cybercrime are reflected in Canada's broader foreign policy. As cybercrime is international in nature, additional engagement with

[58] Note: In-house training is being supported through existing resource levels.

international partners has been undertaken. Through contribution funding, GAC provides technical assistance to foreign countries to build capacity to combat cybercrime and/or facilitate ratification and implementation of the Budapest Convention. Contribution funding is provided primarily under the terms and conditions of the Anti-Crime Capacity Building Program. The GAC Legal Affairs Bureau, specifically the Criminal, Security and Diplomatic Law Division, is responsible for ensuring that Canadian policy and law are consistent with the requirements of the Budapest Convention and Canada's other international obligations. JLA provides advice to Justice on foreign policy issues arising in mutual legal assistance and extradition requests to and from Canada. GAC is the operational lead with respect to the Protocol of Foreign Criminal Investigations in Canada. It provides legal advice in dealing with sovereignty issues that may arise from cross-boundary cyber cooperation related to the Budapest Convention as well as legal advice on international law issues.

A.5 Logic Model

A diagram of the logic model for the IP21C Initiative is presented in Figure A1, overleaf. It illustrates the relationship between the planned activities and expected results.

Figure A1: Investigative Powers for the 21st Century Initiative Logic Model