Council of Europe Second Additional Protocol to the Convention on Cybercrime on Enhanced Cooperation and Disclosure of Electronic Evidence

Consultations, 2023

Purpose of consultations

- Addressing cybercrime is a top priority of the Government of Canada.
- The Government is reaching out to stakeholders for views on an international treaty recently signed by Canada: the *Second Additional Protocol to the Council of Europe Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence* (Protocol), which aims to address cybercrime and electronic evidence for crimes in general.
- This Protocol would provide law enforcement new tools to better access electronic evidence in other countries to combat crime while at the same time ensuring privacy safeguards.
- The input is intended to allow the Government to:
  - better assess the potential impacts of this Protocol;
  - understand concerns around the tools and privacy protections; and
  - consider the development of any new laws or processes to enable Canada to ratify (officially approve) and implement the Protocol.

Background

- Digital technologies have tremendous benefits, but unfortunately also make certain threats possible.
- Criminals and other cyber threat actors, many of whom operate outside our borders, take advantage of security gaps, low cyber security knowledge, and technological developments to commit crimes.
- They steal personal and financial information, intellectual property, and trade secrets. They disrupt and sometimes destroy computer systems, networks and even infrastructures that are relied on for essential services and a way of life.

What are cybercrimes/cyber-related crimes?

- Cybercrime and cyber-related crimes include offences that:
  - target or aim to damage a device such as a computer (e.g., a virus, computer hacking), a mobile phone or a network, or the data on those devices (technology as the target); or
  - are committed through the use of a device such as a computer or mobile phones, etc. (e.g., child sexual exploitation and abuse material; ransomware extortion) (technology as instrument to commit crimes).
- It can be domestic in origin or transnational.

Challenges in addressing cybercrimes

- Electronic evidence of a cybercrime or cyber-related offence is often stored in more than one country.
- It can be very challenging and slow for investigators globally to use the existing tool of **mutual legal assistance** to obtain electronic evidence in other countries to assist in investigations and prosecutions.
- As a result, only a very small portion of reported cybercrime is leading to prosecutions.
- That is why the Government of Canada is pursuing opportunities, like the Second Additional Protocol, to ensure the safety of Canadians from cybercrime.

Council of Europe Convention on Cybercrime

- Canada is Party to the Council of Europe *Convention on Cybercrime* (aka the "*Budapest Convention*").

- This is an international treaty that provides states that are a party to it with tools to help in the investigation and the prosecution of cybercrimes and cyber-related crimes.

- The Second Additional Protocol, recently signed by Canada, is a new, additional part of the *Budapest Convention* and provides enhanced tools for law enforcement and prosecutions.

Second Additional Protocol

- The Second Additional Protocol provides a framework that would:
  - allow countries to share electronic evidence of a cybercrime and crimes in general;
  - allow a country to seek information directly from a service provider (a telecommunications or social media company) to obtain specific information (e.g., subscriber information such as a name or address); and
  - protect human rights and ensure safeguards for the protection of personal data are in place.

- The Protocol would create a more direct process for requesting electronic evidence, providing alternatives to the mutual legal assistance channels which are generally not well-equipped to handle high volumes of requests requiring expeditious production.

What are the safeguards?

- The Protocol sets out powers and procedures ("measures") that are intended to facilitate the prevention, detection, investigation and prosecution of cybercrime. These measures can impact rights.
- Importantly, the Protocol also sets out conditions and safeguards to provide for the protection of human rights and fundamental freedoms, and requirements to protect privacy and personal information, such as placing restrictions on the purposes for which data obtained can be processed and used; limiting onward sharing; ensuring that personal data is only retained for as long as necessary; ensuring access by any individual to data pertaining to them; requiring appropriate data security; and requiring independent oversight.
- The safeguards are some of the most robust found in an international criminal justice treaty and Canada is not restricted from applying further safeguards.
- The Protocol includes provisions aimed at guarding against prejudicial impacts, such as unlawful discrimination.
- Where stronger, Canada's federal and provincial privacy laws would also apply with respect to the possession, use and protection of personal data in criminal investigations.

Reservations in the Second Additional Protocol

- The treaty allows Parties to exercise specific **reservations**. Reservations allow the Party to "opt out" of specified provisions at the time of ratification.
- Canada can opt out of permitting **direct access** by competent authorities (law enforcement) in other Parties to subscriber information held by Canadian service providers (Article 7).
- Opting in or out would have **reciprocal consequences**: if Canada does not create a regime for competent authorities in other Parties to directly obtain such data in Canada, Canadian law enforcement would not be permitted to directly request such data from foreign service providers.
- Canada's approach to this reservation needs to consider that administration of justice is an area of shared jurisdiction.

Signature and ratification

- Canada's signing of the Second Additional Protocol signals its commitment to the spirit and intent of this important initiative. Signing does not, however, bind Canada.

- Canada is only *legally bound* if it **ratifies the Protocol,** subject to any reservations specified**.**

- A decision about whether to ratify the Protocol will be taken by the Government in the future.

- Engaging with Canadians is important to inform next steps on how the treaty could be implemented in Canada.

Some Specific Issues Being Considered

- The Government is seeking feedback on what type of authorization (e.g., judicial or other) Canada should require for investigators **internationally and domestically** to obtain different types of data for criminal justice purposes from internet service providers, including:
  - subscriber information (e.g. name, address, phone number, and billing address), domain name registration data, stored content, and transmission (traffic) data.
- The Government is also seeking feedback about whether Canada should opt out of permitting **direct access** by the competent authorities (law enforcement) of other Parties to subscriber information held by Canadian service providers (Article 7).

Expected outcomes

- If Canada ratifies the Protocol, it is expected to help in the investigation and the prosecution of cybercrimes and cyber-related crimes and other serious crime by:
  - enhancing timely access to electronic evidence for use in the investigation of cybercrime, cyber-related crime and other serious crimes while maintaining robust data protection and human rights safeguards.
  - reducing pressure on Canadian mutual legal assistance channels; and
  - Contributing to the elimination of “safe havens” for electronic evidence and increasing the ability for Canada and its global partners to hold offenders accountable.

Contacts – Department of Justice

- Gareth Sansom, Deputy-Director, Criminal Law Policy Section
- Kimberly Burnett, Senior Policy Analyst, Criminal Law Policy Section
- Phaedra Glushek, Counsel, Criminal Law Policy Section

CSAP-DPA@justice.gc.ca