Council of Europe Second Additional Protocol to the Convention on Cybercrime: Practical Implications for Prosecutors

Organised by the Council of Europe and
the International Association of Prosecutors
May 30, 2024

Gareth Sansom – Department of Justice Canada

Canada's Process: Steps toward Implementing and Ratifying the 2AP

- **Phase 1: Summer 2023 to May 2024**
- The Government of Canada reached out to stakeholders for views on the *Second Additional Protocol to the Council of Europe Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence* (2AP or the Protocol), signed by Canada in June 2023 (see Website on last slide)
- 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.

Canada's Process: Steps toward Implementing and Ratifying the 2AP

Phase 1: Summer 2023 to May 2024

Identified various stakeholder groups in Canada:

- Law Enforcement (federal and provincial)
- Prosecutors
- Private Sector (Service Providers)
- Civil society
- Advocacy NGOs for Victims/Survivors of Cybercrime
- Federal and Provincial Privacy Commissioners

- Conducted a series of online and in-person meetings with stakeholders
- Invited and received written submissions from various organizations from the above stakeholder groups

Policy Development Process

Phase 1: Summer 2023 to May 2024

- Analyzed specific provisions of the 2AP to explore policy options
- Consulted on specific provisions with federal legal counsel who have expertise in specific areas (including privacy, human rights, retention of records, international law, treaty law)
- Analyzed (a) records of discussion from consultation meetings and (b) written submissions from stakeholder groups
- Assessment of whether existing domestic legislative and other measures meet the requirements of each of the provisions or whether new legislation and/or other measures are required

Toward Implementing the Protocol

Considerations

- What is the relevant domestic context with respect to this procedural power?
  - Is it covered by existing legislation and/or other measures?
  - Is there relevant jurisprudence (such as Supreme Court decisions)?
- What legislative or other measures are needed for **outgoing orders**?
- What legislative or other measures are needed for **incoming orders**?

Chapter II, Measures for Enhanced Co-operation: Article 6

- Article 6 establishes procedures for **direct requests** between competent authorities of one Party and an entity providing domain name registration services in another Party to obtain **domain name registration information**.
- This is meant to provide an effective and efficient way to obtain information to identify or contact the registrant of a domain name without using an intermediary or resorting to a compulsory Order.
- Article 6 requires State Parties to use existing measures, or adopt new ones, to:
  - empower its competent authorities (e.g., law enforcement) to issue a request for domain name information to an entity in another State;
  - permit entities providing domain name services to provide domain name information to competent authorities in another State.
  - these are treated as **non-binding requests** (ER para.77)
- It also sets out the information that, at a minimum, must be provided by an authority issuing a request is outlined (e.g., details of the competent authority, the domain name about which information is sought, etc.).

Considerations - Article 6

The Protocol regards “domain name registration data” as different from “subscriber information”, as is evident from the fact that there is an Article 6 and Articles 7 and 8.

There are three schools of thought on the status of domain name registration data:

1. **A domain name is akin to a telephone number or address** that we use to reach a particular entity and does not have value in and of itself.
2. **A domain name is a special property right**. Domain names can be sold or transferred for use (they are a form of intangible property)
3. **A domain does not represent any special type of ownership of an intangible asset, and its registration is carried out on the basis of a contractual relationship between the registrar and the registrant**

- There may be court decisions in different countries that affirm one (or more) of these schools of thought.
- Are there policy considerations regarding the implementation of Article 6 that indicates that some domain name registration data is akin to business registration data and not attract a reasonable expectation of privacy? In what ways is it less than or equal to “subscriber information”?

Considerations - Article 6

- There are different types of domain names: generic top-level domains (gTLDs) and country code top-level domains (ccTLDs). **Article 6 is intended to apply to both ccTLDs and gTLDs** (ER para.80)
- **gTLDs** are more “theme-based” and feature a minimum of three letters. For example, .com was, at one time, most closely associated with businesses, while .org is commonly used by non-profits, and .edu is intended for educational institutions.
- **ccTLDs** are two-letter top-level domains, usually reserved for a specific country, sovereign territory or geography (e.g. .ca).

Considerations - Article 6

- Some ccTLDs have a set of “presence requirements” that only allow (natural or artificial) persons who are residents of that country to register a domain.
- Example: the ***Canadian Internet Registration Authority (CIRA)*** is not a “registrar” it is a “registry”
- There are Canadian presence requirements for registrars and registries with respect to the .ca domain space
- https://www.cira.ca/en/resources/documents/domains/canadian-presence-requirements-registrants/
- https://www.cira.ca/en/resources/documents/domains/canadian-presence-requirements-registrars/
- Are there policy considerations regarding the implementation of Article 6 with respect to incoming requests from another Party when those requested Party’s ccTLD?

Considerations - Article 6

- Domain name registration data in certain cases "**may be personal data** and may be protected under data protection regulations in the Party where the respective entity providing domain name registration services (the registrar or registry) is located or where the person to whom the data relates is located"(ER, Para. 75)
- Are there policy, legal or Constitutional considerations regarding the implementation of Article 6 in those cases where there is a reasonable expectation of privacy associated with the domain name registration data?

Article 14 in relation to the Procedural Powers in the Protocol

- 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 a Party is not restricted from applying further safeguards.
- The Protocol includes provisions aimed at guarding against prejudicial impacts, such as unlawful discrimination.
- Where stronger, a Party's privacy laws would also apply with respect to the possession, use and protection of personal data in criminal investigations.

Next Section:

Articles 7 and 8

Considerations - Article 7

- **Key Features:**
- Direct disclosure
- Voluntary request unlike Article 8 (which is compelled disclosure)
- **Pros:** (law enforcement/victims) ability to investigate and prosecute more swiftly criminal offences that have digital evidence
- Relieves pressure from existing Mutual Legal Assistance channels. (could expand bullet)
- **Cons:** how to ensure protection in accordance with the Constitutional (Charter) Rights and Freedoms, including measures to mitigate and safeguard privacy risks associated with personal data?

Chapter II, Measures for Enhanced Co-operation: Article 7

- Article 7 sets out the procedure for **direct co-operation** between a competent authority of one Party and a service provider in another Party to obtain subscriber information

- Article 7 is **not mandatory**; a Party to the Protocol could take **a reservation**. This would have reciprocal consequences (comity): The reservation would **prevent** that Party as well as the other Party's law enforcement or competent authorities from **directly requesting/demanding subscriber information.** Such Parties would fall back on Article 8.

- **Making a declaration** under Article 7 (2)(b), a Party could require oversight by a **prosecutorial, judicial, or independent authority** at the time of ratification.

- A Party may choose to require notification (para 5(a)): if so, the Requesting Part must notify the specified authority in the requesting Party as well as the competent authority that requested the information
- Whether or not notification is asserted, a Party's service providers may be required to consult with the specified authorities prior to disclosure (para 5(b))
- One rationale of Para 5(a) or(b): A Party implementing Article 7 would specify an authority to monitor requests under Article 7 to ensure that there are not conflicting law enforcement activities and ensure the appropriate law enforcement activities are prioritized (aka "de-confliction")

Considerations - Article 7

- **Scope:** given the definition of "subscriber information" in the Budapest Convention, what is "in scope" in terms of "subscriber information"?
- How expansive might this be and could there be differences between Parties as to what is in an out of scope?
- How would such differences be handled in a direct request regime?
- **Important Policy Options:**
- Take a reservation on Article 7 as a whole
- **"Fine tune"** Article 7: Potential reservation under Art 7(9)(b) and declarations Art 7 (2)(b) and (5)(a) and/or (b)

Rationale: *Why do we need Art. 8?*

- **Subscriber information (SI) –** Most often sought information in criminal investigations relating to cybercrime and other crimes involving electronic evidence.
- **Traffic data** - also often sought in criminal investigations - rapid disclosure may be needed to trace source of a communication.
- Many Parties require Mutual Legal Assistance (MLA) requests to obtain this type of data for a Requesting Party.
- MLA regimes are generally not well-equipped to handle high volumes of requests requiring expeditious production.

Rationale – cont'd

- Art. 18 of the *Convention on Cybercrime (Convention)* addresses some aspects of obtaining SI, but additional tools that provide for faster access **through a compelled process** were deemed necessary under the Protocol

- Article 8 is designed to be a more streamlined process:
  - ✓ Less information required than under MLA;
  - ✓ Disclosure is expected to be much faster;
  - ✓ Supplements MLA process.

Chapter II, Compelling service providers: Article 8

- **Article 8** requires Parties to empower their competent authorities (e.g., judicial, administrative or other law enforcement authority) to issue an Order to another Party **to compel** a service provider to produce specified and stored subscriber information or traffic data for the purpose of specific criminal investigations or proceedings.

- Compelling a service provider is done through mechanism of the **requested Party's choice** (e.g., issuing production order or endorsing requesting Party's Order).

- A Party may **reserve** the right not to apply Article 8 to traffic data (para 13).

- **Article 8** also sets out service standards, and return/notification/processes for non-compliance i.e.:
  - twenty days for subscriber information; and forty-five days for traffic data.
  - if the requested Party cannot comply in the manner requested, it shall promptly inform the requesting Party, and (if applicable) specify conditions under which it could comply.
  - the requested Party can refuse or postpone compliance.

Considerations - Article 8

- **Key Features:**
- Federal competent authority receives request from the other Party
- Compelled disclosure of an order unlike Article 7 (voluntary request)
- **How could Article 8 be implemented?**
- How will Article 8 expedite Mutual Legal Assistance in Canada?
- **Question:** Policy option: Extend Article 8 to “traffic data”?

Example: Canadian Considerations – Articles 6- 8

- Canada can specify what type of authorization would be required for investigators both **internationally and domestically** to obtain different types of data for criminal justice purposes from Canadian ISPs.
- Through consultations, Canada sought feedback on potential new "made for purpose" authorizations.

	Type of Data	Canadian Requirements
Existing Procedural Powers	(Stored) Content data	Prior judicial authorization (threshold = reasonable grounds to believe); aka **general production order (487.014)**
	Transmission (aka traffic) data	Prior judicial authorization (threshold = reasonable grounds to suspect); aka **transmission data production order (s. 487.016)**
New "Made for Purpose" Procedural Powers	Subscriber Information	Authorized under reasonable "lawful authority" or warrantless in exigent circumstances [e.g., R v. Spencer (2014)]
	Domain name registration data	An explicit provision would resolve a process that varies domestically and continues to evolve globally

Canada – Consultations - Background

- **Canada: Fall 2023-Spring 2024 Consultations on the**

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

- **English**

https://www.justice.gc.ca/eng/cj-jp/cyber/index.html

https://www.justice.gc.ca/eng/cj-jp/cyber/id-di/index.html

- **French**

https://www.justice.gc.ca/fra/jp-cj/cyber/index.html

https://www.justice.gc.ca/fra/jp-cj/cyber/di-id/index.html