Communications Security Establishment | Centre de la sécurité des télécommunications

OPERATIONAL POLICY

OPERATIONAL POLICY
OPS-1-16

Policy on Metadata Analysis for Foreign Intelligence Purposes

Effective Date:

January 7th 2016

Canada

1. Introduction

1.1. Objectives

The objectives of this policy are to provide the governing principles for metadata analysis activities conducted under Part (a) of CSE's mandate.

1.2. Context

Metadata is defined in the *Ministerial Directive on the Collection and Use of Metadata* (Metadata MD) as "information associated with a telecommunication to identify, describe, manage or route that telecommunication or any part of it as well as the means by which it was transmitted, but excludes any information which could reveal the purport of a telecommunication, or the whole or any part of its content."

Metadata analysis is authorized under CSE's foreign intelligence (FI) mandate and is used to:

- Enable the discovery of foreign targets and produce foreign intelligence (FI) in support of Government of Canada intelligence priorities;
- Conduct network analysis; and
- Facilitate cyber threat detection.

1.3. Authority to Conduct Metadata Analysis

CSE's authority to conduct metadata analysis comes from its mandate in the *NDA* to acquire and use information from the global information infrastructure (GII) for the purpose of providing FI. Metadata analysis activities undertaken by CSE under Part (a) of the mandate are carried out:

- Under the authority of paragraph 273.64(1)(*a*) of the *National Defence Act* (*NDA*);
- Subject to the restrictions set out in subsection 273.64(2) of the *NDA*; and
- In accordance with all relevant Ministerial Directives (MDs), including but not limited to the:
  - *MD on the Use and Collection of Metadata;*
  - *MD on the Privacy of Canadians;*
  - *Accountability Framework; and*
  - *MD on Intelligence Priorities.*

1.4. Application

This policy applies to CSE personnel and other parties (including secondees, integrees, contractors, students and CFIOG personnel) conducting activities under Part (a) of CSE's mandate.

2. Policy

2.1. Preamble

The diversity of CSE's metadata analysis activities is such that the specific considerations of each cannot be covered in this policy. Any metadata analysis activities conducted under Part (a) that have not been explicitly outlined in this policy must conform to Canadian law and the principles outlined herein.

The subsequent chapters of this policy address the following metadata analysis activities:

- **Chapter 3:** Metadata Analysis for Foreign Intelligence Purposes
- **Chapter 4:** Network Analysis and Prioritization
- **Chapter 5:** Metadata Analysis [redacted]

2.2. Principles

The following principles guide this policy:

- Any metadata analysis activities (or proposed activities) that may constitute an elevated risk to the privacy of Canadians must be approved by management and consulted with the relevant policy teams, as appropriate, and must be subject to measures to protect the privacy of Canadians or persons in Canada in the use and retention of the information.
- Metadata analysis must not be directed at Canadians or at persons in Canada. In the absence of indications that an identifier is used by a Canadian, it can be used for metadata analysis;
- Identifiers used by a Canadian anywhere or a person located in Canada cannot serve as the focus of an FI activity using metadata that CSE has acquired for foreign intelligence purposes;
- Identifiers used by a Canadian or person in Canada must be protected from inadvertent targeting (e.g., be entered as a Protected Entity in the target knowledge database), and no activities may be directed at the identifier while it is being used by a Canadian or person in Canada;
- Network analysis [redacted] is subject to additional oversight to ensure adequate privacy protection measures are in place; and
- Metadata analysis [redacted] the proper approvals are obtained.

3. Metadata Analysis for Foreign Intelligence Purposes

3.1. Preamble

This chapter outlines the process for conducting metadata analysis for the purpose of foreign intelligence, including target development and threat discovery.

3.2. Conditions for Metadata Analysis

In cases where the nationality or location of the user of an identifier is difficult or not possible to determine because the person is using a non-specific identifier (e.g., a ".com" web email address), and in the absence of information to suggest that the identifier is used by a Canadian or person in Canada, the identifier can be assumed to be under foreign control. If there is information that the user of an identifier is Canadian or person in Canada, the identifier must be protected from any further activities.

The following table summarizes the conditions under which person-person communications can be analyzed for FI purposes.

Type	User 1	User2	Analysis Permitted?
Person-Person	Foreign	Foreign	Yes
Person-Person	Foreign	Canadian	Yes (of foreign user only)
Person-Person	Canadian	Canadian	No
Person-Many	Foreign	Many	Yes
Person-Many	Canadian	Many	No

Some identifiers, however, must be presumed to be used by a Canadian (e.g., email addresses ending with .ca or phone numbers beginning with a Canadian area code; hereafter "Canadian" identifiers) unless there are reasonable grounds to believe that the identifiers are being used by a foreign entity located outside Canada.

3.3. **Identifiers that Appear Canadian**

Prior to conducting metadata analysis using identifiers that appear Canadian, analysts must have reasonable grounds to believe that the users are not Canadian or persons in Canada. Once a foreign use of an identifier is established (to the extent possible), metadata analysis using the identifier is permissible, provided analysts receive permission to conduct metadata analysis on these identifiers from their supervisors. Analysts must detail the nature of the corroborating information used to establish foreign control of the identifier.

Reasonable grounds to believe that an identifier that appears Canadian is under foreign control can include (but is not limited to):

- [redacted]
- Intelligence from HUMINT sources;
- Citizenship checks;
- [redacted]
- Open source information;
- [redacted]
- Any combination of the above.

Supervisors are responsible for maintaining a copy of the documentation detailing their rationale for approval or refusal of a request to analyze an identifier that appears Canadian but is reasonably expected to be used by a foreign person outside Canada. This documentation must be maintained for a minimum of [redacted] for audit and review purposes.

Example: If an identifier is hosted by a Canadian organization (e.g., an email address with a Canadian university's domain, user@CanadianUniversity.ca) but the sole user is a foreigner located outside Canada, metadata analysis of the identifier is permitted, if approved by the supervisor. The analyst may proceed with the analysis having documented the following:

- The domain is associated with a Canadian organization; it is likely that many of the communicants interacting with that identifier have Canadian status (in the example above, the communicants could be members of the university community located in Canada); and
- [redacted]

3.4. **Identifiers** [redacted]

3.5. **Multi-User Identifiers** To help mitigate risks to the privacy of Canadians, consult Corporate and Operational Policy for advice on how to handle multi-user identifiers where a Canadian may be a potential user, such as shared handsets or IP addresses of foreign internet cafés frequented by Canadians.

3.6. **Advice and Responsibility** Corporate and Operational Policy will provide guidance on how to best deal with identifiers where there is an increased potential risk to the privacy of Canadians. Corporate and Operational Policy will provide guidance as an advisor, not an approval authority.

The responsibility for metadata analysis activities lies with the decision maker electing to undertake the analysis, as per the approval authorities outlined in Chapter 6.

3.7. **Contact Chaining** Contact chaining is the process of analyzing an identifier to determine the nature of the user's communications (e.g., contacts, duration and time of communications events), [redacted]

Analysts must not deliberately direct their activities at Canadians (or persons in Canada) under any circumstances. [redacted]

3.8. [redacted] **Identifiers**

Analysts are permitted to [redacted] identifiers of foreign entities located outside Canada for targeting and analytical purposes. [redacted]

3.9. **Target Discovery and Development**

Other types of metadata analysis aimed at facilitating target discovery or SIGINT development are permitted, provided that the analysis is not directed at Canadians or persons in Canada. Metadata analysis activities for target discovery and development may include, but are not limited to:

[redacted]

3.10. **End Product Reports**

End product reports based on metadata analysis must focus on the foreign subjects of the analysis.

Any identifiers used by a Canadian or person in Canada that are to be included in an end product report must be suppressed in accordance with *OPS-1-7, Operational Procedures for Naming in SIGINT Reports*.

4. Network Analysis and Prioritization

4.1. **Overview**

Network analysis and prioritization pertains to developing methods for understanding the GII in order to identify communication links of interest to meet Government of Canada (GC) FI priorities. Understanding networks enables CSE to [redacted] identify and target entities of FI importance to the GC.

From a network analysis perspective, the GII consists of events and infrastructure. [redacted]

4.2. [redacted]

Analysis [redacted] is to be conducted in accordance with *OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*.

[redacted]

4.3. [redacted]

[redacted] Analysis [redacted] must be conducted in a manner that is not directed at Canadians or persons in Canada and must be in accordance with *OPS-1: Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSE Activities*.

[redacted]

4.4. Oversight and Approval

Prior to conducting network analysis of a [redacted] involving Canadian networks, analysts must provide a rationale to their managers detailing:

- The purpose of the analysis;
- Rationale for why the analysis must include the Canadian network;
- The anticipated benefit of the analysis;
- The assessed risk to the privacy of Canadians; and
- What measures will be taken to mitigate the risk of violating the privacy of Canadian users (e.g., anonymizing identifiers).

Operational managers are responsible for maintaining a copy of the documentation detailing their rationales, approvals, or refusals for a minimum of [redacted] for audit and review purposes.

5. Metadata Analysis [redacted]

5.1. Context

[redacted]

5.2. Approval Process for [redacted]

The following table summarizes the conditions under which [redacted] identifiers can be analyzed.

Identifier	Pre-Approval Required	Approval Authority	Requirements
[redacted]			

5.3. Validity and Re-approval

[redacted]

5.4. **Analysis**

[redacted]

[redacted]

Note: Contact Corporate and Operational Policy for guidance. [redacted]

5.5. **Use and Dissemination**

Reporting derived from metadata analysis [redacted] identifier is permitted, provided that:

- The report does [redacted] identifier; and
- The report dissemination is limited (see *CSOI-4-1, SIGINT Reporting*).

Analysts and operational managers should take into account the nature of the material they are sharing when releasing a report based on the results of analysis of a [redacted] identifier. [redacted]

[redacted]

5.6. **Report Release**

The Director General Intelligence (DGI) is the approval authority for releasing reports based on the results of metadata analysis [redacted]

6. Approval Authorities

6.1. Accountability for Activities

The following table outlines accountabilities for conducting metadata analysis of identifiers used by Canadians, persons in Canada, [redacted]

Role	Responsibility
Deputy Chief, Policy and Communications	Approves exceptional requests to this policy
Director General Intelligence	[redacted]
Director, Operational Area	
Operational Manager	• Retains records of rationales, approvals, re-approvals and refusals for a minimum of [redacted] [redacted] • Retains records of rationales, approvals, re-approvals and refusals for a minimum of [redacted] [redacted] • Retains records of rationales, approvals and refusals for a minimum of [redacted]
Operational Supervisor	Makes the decision on analysis of: • Identifiers that appear Canadian but are under foreign control (including email addresses hosted by Canadian domains under foreign control, [redacted] Retains records of rationales, approvals and refusals for a minimum of [redacted]

7. Additional Information

7.1. Policy Approval

This policy was approved by the Policy Committee on (date).

Minor amendments may be approved by Director, Disclosure, Policy, and Review.

7.2. Exceptions to OPS-1-16

The Deputy Chief, Policy and Communications (DC PolCom) may approve exceptions to this policy.

Requests for exceptional authorizations must be submitted to Corporate and Operational Policy and will present rationales outlining:

- The reason for the exception (i.e., why the request falls outside the scope of this policy);
- The operational need that justifies the exception; and
- The impact of the request on the privacy interests of the Canadian or person in Canada.

Approvals are granted at the discretion of DC PolCom if and when satisfied that the request meets the above criteria.

7.3. Amendment Process

Situations may arise where amendments to this policy are required due to changing or unforeseen events. Amendments will be made in accordance with *ORG-1* and *ORG-1-1*. They will be communicated to staff and posted on the Corporate and Operational Policy website.

7.4. Review Process

All CSE activities, including policies and procedures, are subject to management monitoring, internal and external audit and review by various government review bodies, including the CSE Commissioner and the Privacy Commissioner.

7.5. Consequences of Non-Compliance

The Chief is responsible for taking corrective measures with those CSE personnel found to be in violation of this policy. Corrective measures can range from training, to the suspension or removal of delegated authority, to taking disciplinary action, or any combination of these measures.

7.6. References

- *Canadian Charter of Rights and Freedoms*
- *National Defence Act*
- *Privacy Act*
- *Criminal Code*
- *Ministerial Directive on the Privacy of Canadians*
- *Ministerial Directive on the Collection and Use of Metadata*
- *Ministerial Directive on CSE's Accountability Framework*
- *Ministerial Directive on Intelligence Priorities*
- *CSE Ethics Charter*
- *OPS-1, Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
- *OPS-1-7, Operational Procedures for Naming in SIGINT Reports*
- *SPI-2-14, SIGINT* [redacted] *Data*

7.7. Questions

Questions regarding this policy should be addressed to Corporate and Operational Policy (d2policyadvice@cse-cst.gc.ca).