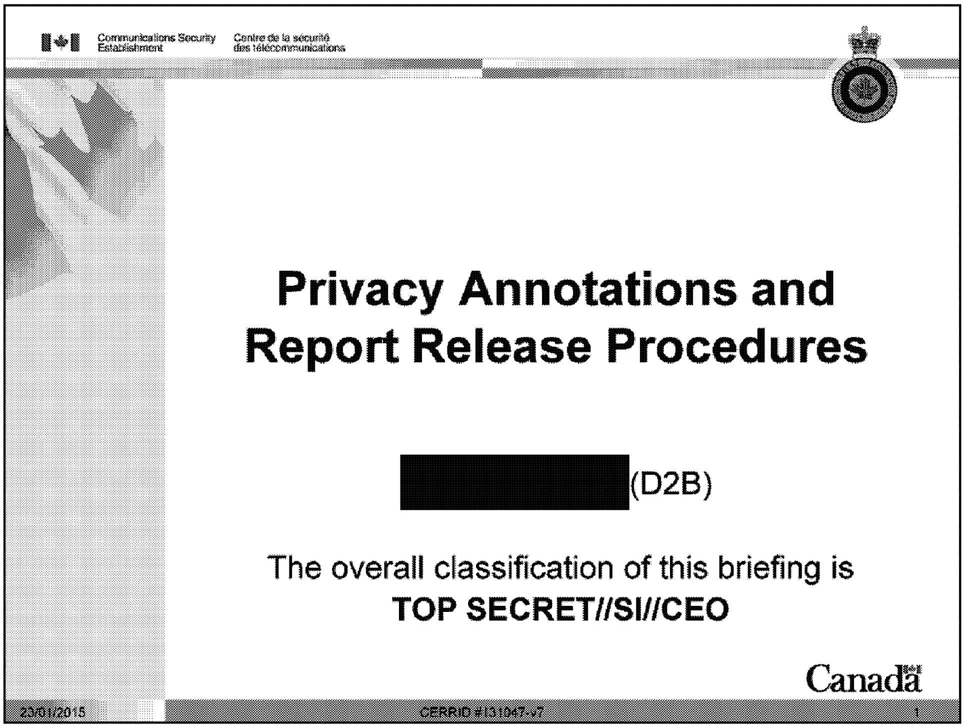


Communications Security Establishment
Centre de la sécurité des télécommunications

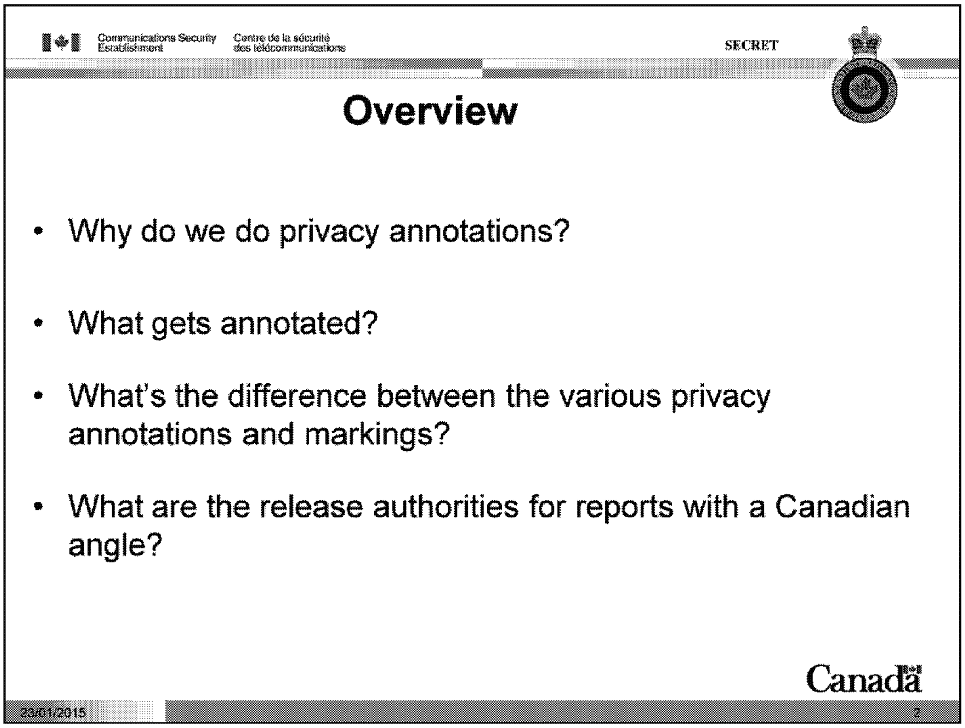
Privacy Annotations and Report Release Procedures

[redacted] (D2B)

The overall classification of this briefing is
TOP SECRET//SI//CEO

Canada

23/01/2015 CERRID #131047-v7 1



Communications Security Establishment
Centre de la sécurité des télécommunications

SECRET

Overview

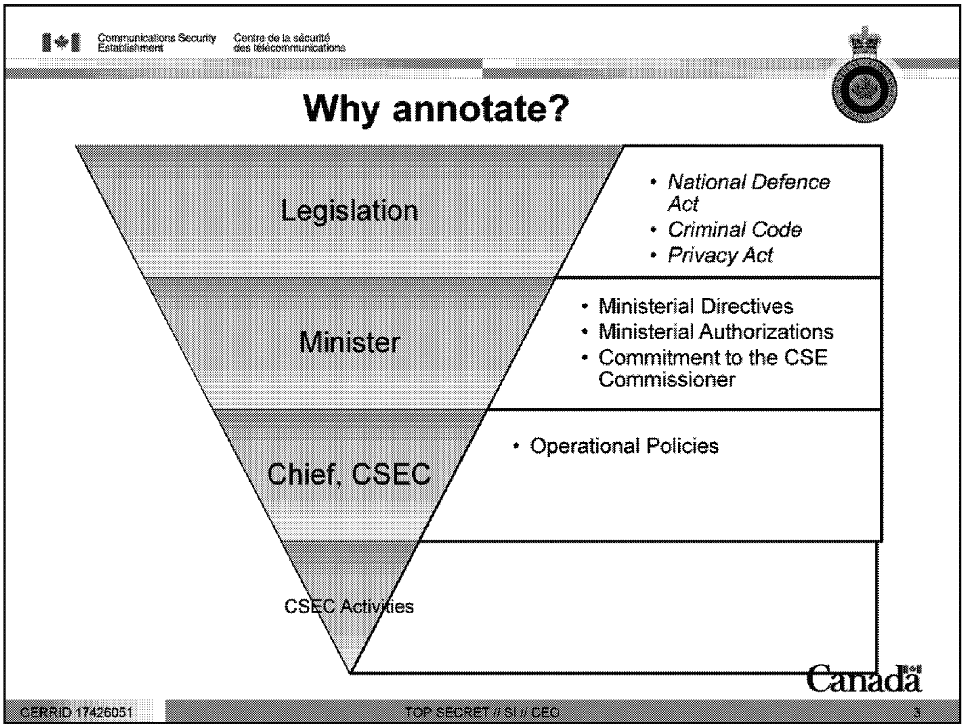
- Why do we do privacy annotations?
- What gets annotated?
- What's the difference between the various privacy annotations and markings?
- What are the release authorities for reports with a Canadian angle?

Canada

23/01/2015

2

- Our intent is to help you understand why you are obliged to make privacy annotations and markings.
- I will be covering a lot of material this afternoon. You don't need to remember it all – the key is to remember the concepts. We've also developed tools to help you determine how to annotate the traffic.
    - Ultimately, if you understand why the rules are there, you are better able to apply them appropriately.
- Please feel free to ask questions as we go along. I'll also have some time at the end to answer any questions.



Communications Security Establishment Centre de la sécurité des télécommunications

Why annotate?

- *National Defence Act*
- *Criminal Code*
- *Privacy Act*

- Ministerial Directives
- Ministerial Authorizations
- Commitment to the CSE Commissioner

- Operational Policies

CERRID 17426051 TOP SECRET // SI // CEO 3

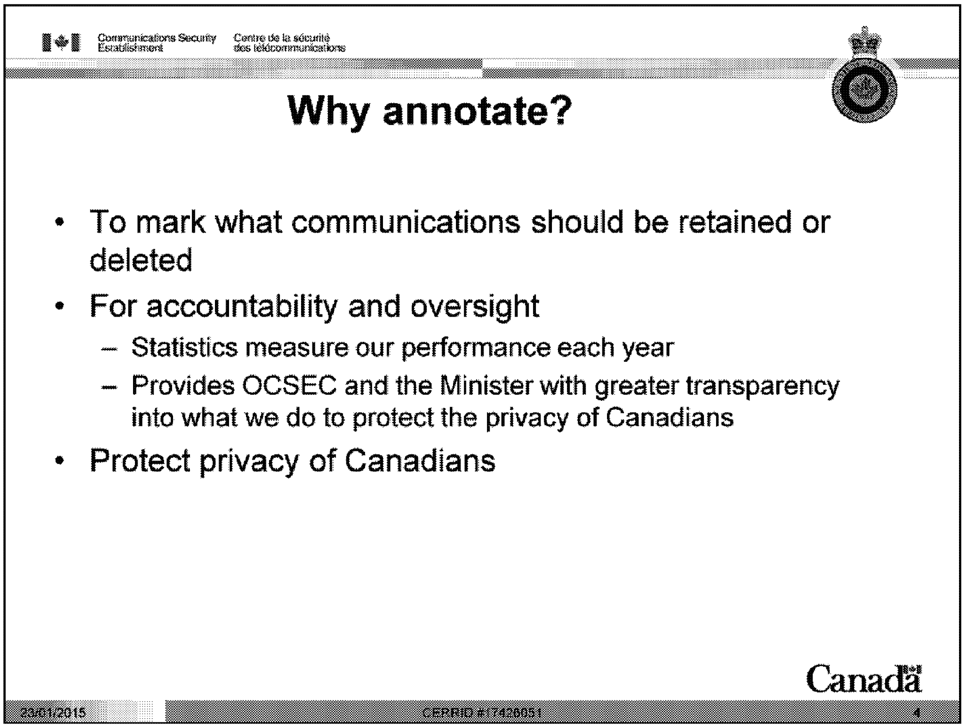
- Under the National Defence Act, CSEC is prohibited from directing its activities at Canadians anywhere or at any person in Canada. Further, CSEC's activities are subject to measures to protect the privacy of Canadians in the use and retention of intercepted information.
- The National Defence Act, provides the Minister with two key tools to direct and enable CSEC activities: **Ministerial Directives and Ministerial Authorizations**.

- **MDs** are written directions from the Minister to the Chief CSEC respecting how he is to carry out of his duties and functions.
- They may relate to a specific program or activity (e.g. MD on [redacted], or to the Minister's general expectations for CSEC activities (e.g. the MD on Accountability).
- The MD on the Privacy of Canadians was updated in November 2012 and contains specific instructions on how the Minister expects CSEC to protect the privacy of Canadians in the conduct of its activities.

- Next are **MAs**.
- The interception of a private communication is prohibited under the *Criminal Code.* The problem is that CSEC cannot eliminate entirely the risk of incidentally intercepting a private communication in the course of its mandated SIGINT or ITS activities. (For example, we cannot know in advance that a targeted foreign entity will not communicate with a Canadian or a person in Canada.)
- MAs are, therefore, required for any activity where there is a risk of intercepting private communications under Part A or B of the mandate. You can think of an MA as a shield from prosecution in the event that CSEC intercepts a private communication.
- Ministerial Authorizations relate to a specific activity or class of activities (i.e. a specific method of acquiring foreign SIGINT or protecting computer systems) rather than to a specific operation or target. They last for a maximum of one year.
- Should operational requirements exist beyond this, CSEC must request a new Ministerial Authorization to continue an activity that risks the incidental interception of private communications.

- Before the Minister can issue an MA for an activity, he must be satisfied that certain conditions have been met, including specific measures to protect the privacy of Canadians. The pre-conditions for SIGINT and ITS MAs are slightly different and are laid out in sections 273.65(2) and (4) respectively.
- CSEC currently has three Ministerial Authorizations that enable its foreign SIGINT collection:
  - [redacted]
  -
  -
- A CSIS warrant is their equivalent of an MA. Warrants permit CSIS to intercept a private communication without breaking the law.
- Before 2001 and the changes to the National Defence Act, CSEC couldn't conduct any collection where private communications might be encountered, such as [redacted]

IRRELEVANT



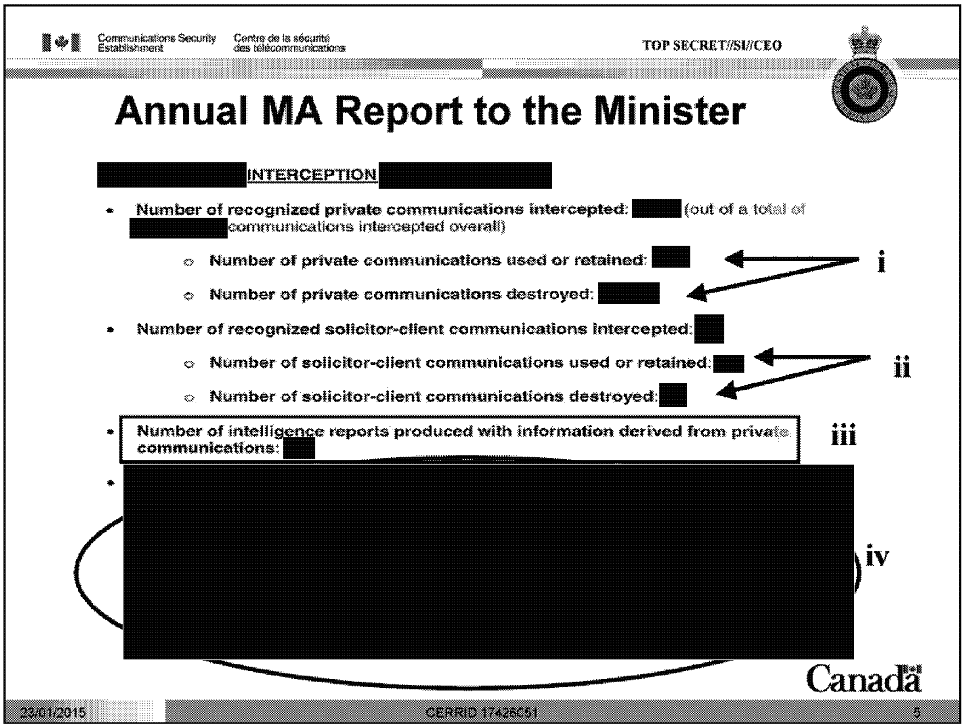
Communications Security Establishment Centre de la sécurité des télécommunications

Why annotate?

- To mark what communications should be retained or deleted
- For accountability and oversight
  - Statistics measure our performance each year
  - Provides OCSEC and the Minister with greater transparency into what we do to protect the privacy of Canadians
- Protect privacy of Canadians

Canada

23/01/2015 CERRID #17426051 4



Communications Security Establishment | Centre de la sécurité des télécommunications | TOP SECRET//SI//CEO

Annual MA Report to the Minister

[redacted] INTERCEPTION [redacted]

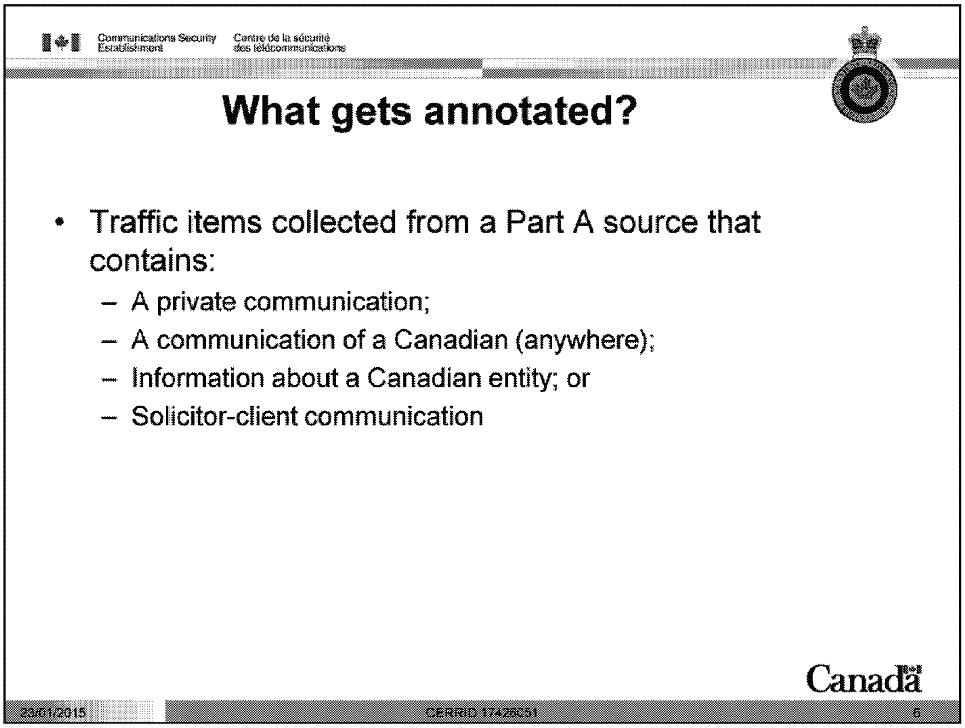
- Number of recognized private communications intercepted: [redacted] (out of a total of [redacted] communications intercepted overall)
  - Number of private communications used or retained: [redacted]
  - Number of private communications destroyed: [redacted]
- Number of recognized solicitor-client communications intercepted: [redacted]
  - Number of solicitor-client communications used or retained: [redacted]
  - Number of solicitor-client communications destroyed: [redacted]
- Number of intelligence reports produced with information derived from private communications: [redacted]
- [redacted]

Canada

23/01/2015 CERRID 17426051 5

- **Within four months of the expiration of an MA we need to report to the Minister on the number of private communications that intercepted and what we did with them.**
- **Here's an example of a on our [redacted] MA. As you can see, we've clearly identified:**
  - The number of recognized private communications that are used or retained;
  - The number of solicitor-client privilege comms that are used and retained;
  - The number of intelligence reports produced from inforatmion derived from private intercepted pursuant to an MA;
  - The FI value of these reports.
- SPOC uses the annotations made by analysts in CSEC traffic databases to generate the required statistics regarding the use and retention of private communications and solicitor-client communications.
- To come up with the stats for number 3, SPOC finds the traffic that has been annotated for retention in the traffic databases and uses the traffic ID number to find the related end-product report in [redacted]
- For the comments under number 4, SPOC will look at the client feedback.
- If traffic has been annotated for retention but wasn't reported, SPOC will call the analyst who made the annotation (using the "viewed by" logs) to ask why it was retained.
- If we can't report accurate numbers to the Minister, or we can't produce these statistics upon request, this will affect whether the Minister is satisfied that the pre-conditions for future MAs have been met. And, if we can't get an MA for an activity, we can't continue to operate those collection methods. Proper annotation matters.

NOTE: CSEC is not required under an MA to report marked [redacted] traffic to the Minister. SPOC reports to the Minister annually on total [redacted] that are being retained for FI purposes).

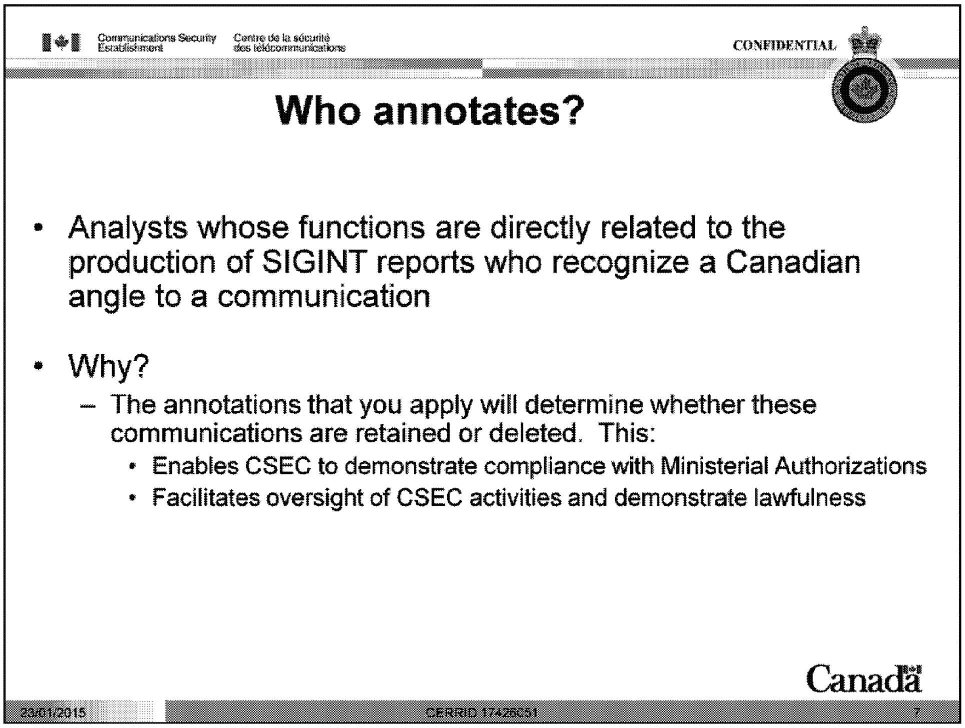


Communications Security Establishment Centre de la sécurité des télécommunications

What gets annotated?

- Traffic items collected from a Part A source that contains:
  - A private communication;
  - A communication of a Canadian (anywhere);
  - Information about a Canadian entity; or
  - Solicitor-client communication

Canada



Communications Security Establishment Centre de la sécurité des télécommunications

CONFIDENTIAL

Who annotates?

- Analysts whose functions are directly related to the production of SIGINT reports who recognize a Canadian angle to a communication
- Why?
  - The annotations that you apply will determine whether these communications are retained or deleted. This:
    - Enables CSEC to demonstrate compliance with Ministerial Authorizations
    - Facilitates oversight of CSEC activities and demonstrate lawfulness

Canada

23/01/2015 CERRID 17425051 7

- All traffic in [redacted] must be annotated when it is recognized as falling into one of four categories:
  - **Private communications**
  - **Communications of Canadians outside Canada**
  - **Solicitor-client communications**
  - **Communications containing information about Canadians**
- **As a quick reminder:**
- **Private Communications** are those where either the originator or the recipient is physically located in Canada
  - The determining factor is GEOGRAPHY, not nationality.
  - Bear in mind, though, that [redacted] are taken into account when making -[redacted]
- The **communications of Canadians outside Canada** are also afforded the same privacy considerations as private communications. So, what is a Canadian?
  - A Canadian citizen or a Permanent Resident
  - A corporation incorporated under an Act of Parliament or of the Legislature of a province; and
  - Canadian organizations, which are accorded the same protection as Canadian citizens and corporations
- There are two criteria for a communication to be considered **solicitor-client**:
  - It must be between a client and a person authorized to practice as a lawyer or a notary in the province of Quebec or as a barrister or solicitor in the rest of Canada – or with any person employed in the office of a lawyer, notary, barrister or solicitor.
  - AND, it must be directly related to the seeking, formulating or giving of **legal advice** or **legal**

assistance.

- There are special handling procedures for solicitor-client communications outlined in OPS-1.

- **Information about Canadians** includes:
  - Any personal information about a Canadian (i.e. information that could identify a person), any business information about a Canadian corporation or any information about a Canadian organization.
  - The two exceptions to this are information about people who have been deceased for 20 years and information related to the position or function of a federal employee.

- So – **<u>who annotates</u>**?
  - Only analysts whose functions relate to the production of SIGINT reports annotate traffic because they are best placed to determine whether a communication that falls into one of these four categories has FI value.
- **<u>When do you annotate?</u>** When you're scanning traffic and something jumps out at you and says **"Canada,"** then you may need to make a privacy annotation.

- **Why does this all this matter?**
  - The annotations you apply to traffic determine whether a communication is retained or deleted. In accordance with Ministerial Authorizations, CSEC can only retain communications that fall into the categories above when they meet specific criteria and we need to report on an annual basis how many of these communications we intercept, how many of these are used or retained, and how many are deleted.
  - The CSE Commissioner will also review CSEC's activities to ensure they comply with the law and appropriately protect the privacy of Canadians. – Proper annotations are important and help CSEC demonstrate its compliance.

[redacted] will explain the "how to" in his briefing

Examples …

Canadian 1 (in Canada) sends message to Foreigner 1 (outside Canada)

= Private Comm

Foreigner 1 (outside Canada) forwards that message to Foreigner 2 (outside Canada)

≠ Private Comm

Comm between two foreigners outside Canada where a [redacted]

≠ Private Comm

Comm from the [redacted]

= Private Comm

Canadian 1 (in Canada) sends message to Foreigner in Canada

= Private Comm **(contact SPOC)**

Communications Security Establishment | Centre de la sécurité des télécommunications

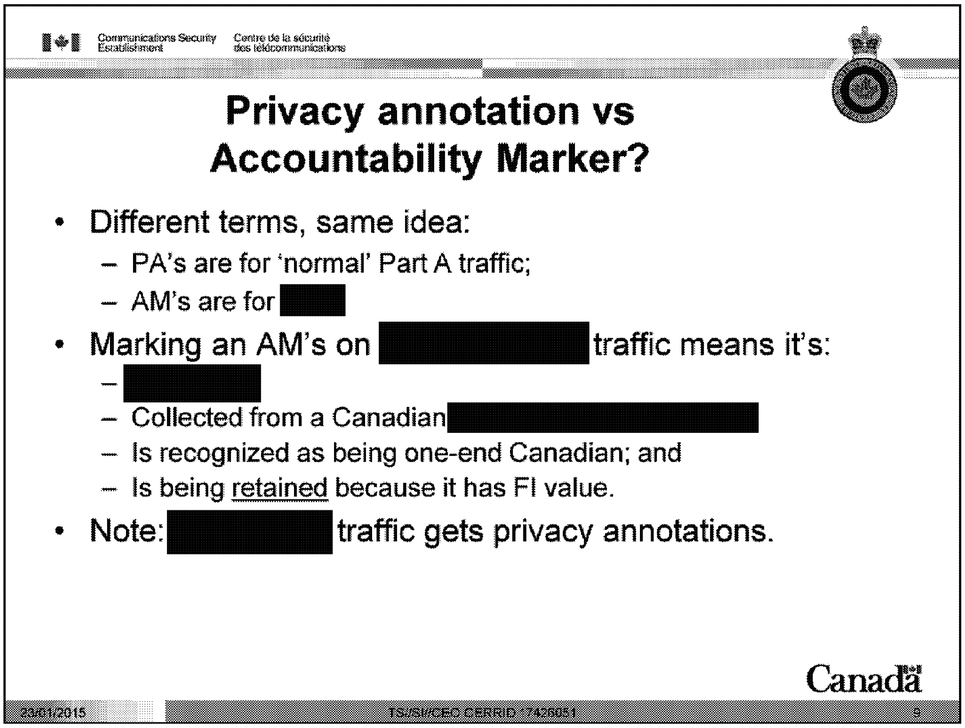
[redacted]

[redacted]

23/01/2015 CERRID 17426051 8

E-mail

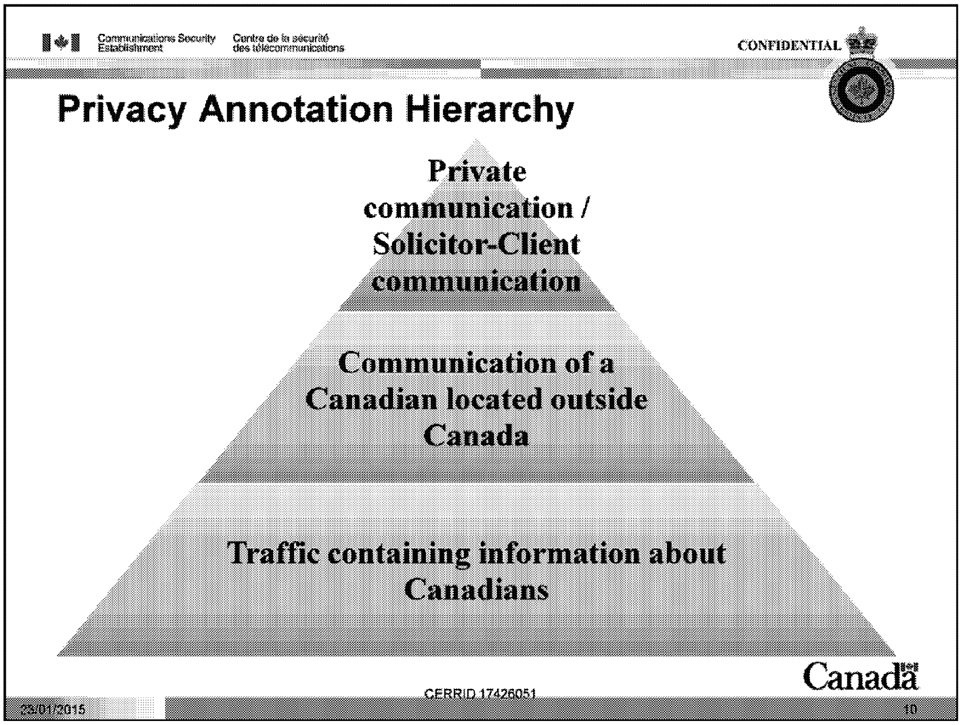
- Here’s an example of an email that’s a private communication.
- What tells you that this is Canadian?
  - [redacted]



Privacy annotation vs Accountability Marker?

- Different terms, same idea:
  - PA's are for 'normal' Part A traffic;
  - AM's are for [redacted]
- Marking an AM's on [redacted] traffic means it's:
  - [redacted]
  - Collected from a Canadian [redacted]
  - Is recognized as being one-end Canadian; and
  - Is being retained because it has FI value.
- Note: [redacted] traffic gets privacy annotations.

Canada



Communications Security Establishment Centre de la sécurité des télécommunications

CONFIDENTIAL

Privacy Annotation Hierarchy

Private communication / Solicitor-Client communication

Communication of a Canadian located outside Canada

Traffic containing information about Canadians

Canadä

CERRID 17426051

23/01/2015

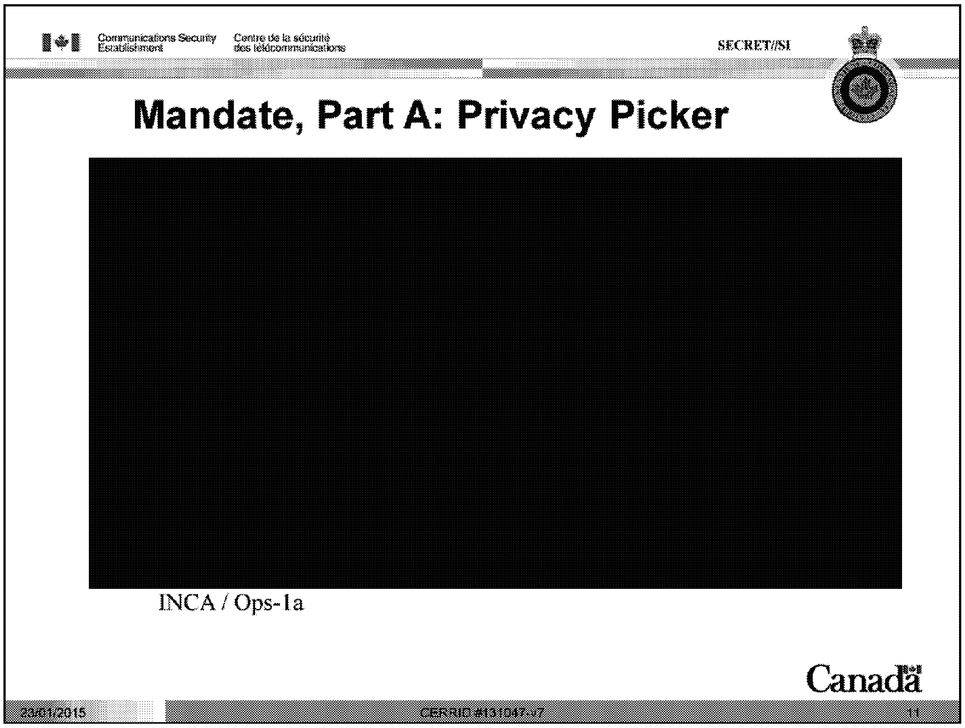
10

- Annotations are mutually exclusive—you shouldn't apply more than one annotation to any piece of traffic.

- This pyramid illustrates the hierarchy of different annotations and can help you determine how to annotate a piece of traffic that falls into more than one category.
  - Private communications and Solicitor-Client communications are at the top
  - Communications of Canadians located outside Canada are next
  - Information about Canadians is next

- The hierarchical order for annotations stems from the origin of the requirement to annotate
  - Requirements under Ministerial Authorizations take precedence over policies.

- So, looking at this pyramid, a communication of a Canadian located outside Canada that also contains information about Canadians should be annotated as a communication of a Canadian located outside Canada.



Communications Security Establishment Centre de la sécurité des télécommunications

SECRET//SI

Mandate, Part A: Privacy Picker

[redacted]

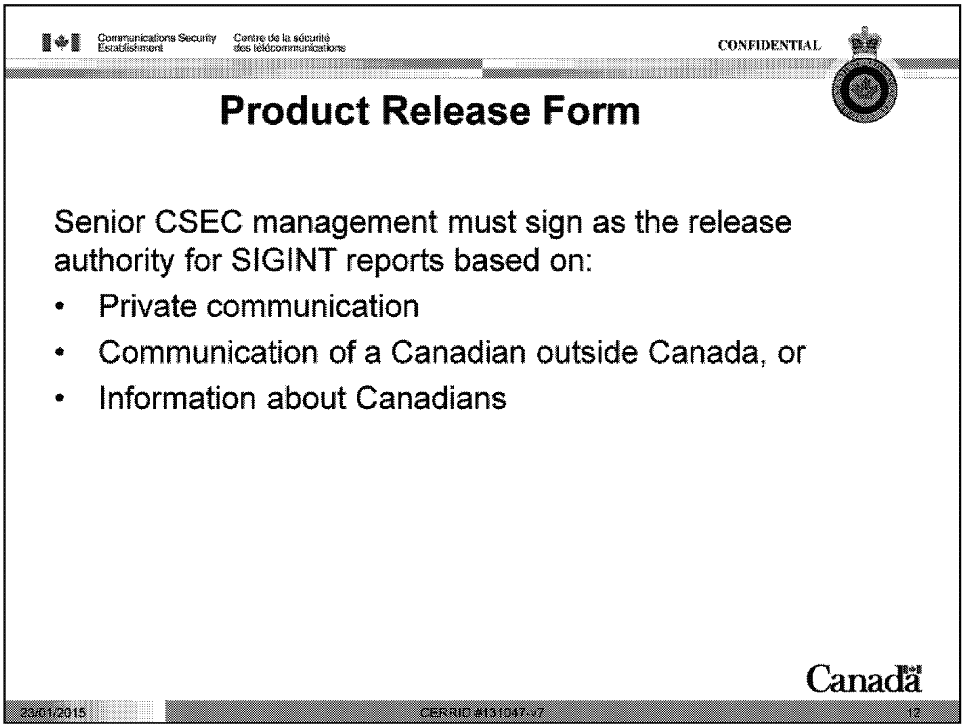
INCA / Ops-1a

Canada

23/01/2015 CERRID #131047-v7 11

- The Privacy Picker is a tool to assist analysts in choosing the appropriate privacy annotation or accountability marking for traffic items they recognize as one-end Canadian or containing information about Canadians.
- This tool is not meant to replace the informed assessment of the analyst, who may have other pertinent information that may alter the proposed annotation and/or OPS category.
- The final decision of how to annotate a piece of traffic remains the responsibility of the analyst.

- This is an example of a completed privacy picker form for a private communication that has foreign intelligence value.



Communications Security Establishment Centre de la sécurité des télécommunications

CONFIDENTIAL

Product Release Form

Senior CSEC management must sign as the release authority for SIGINT reports based on:

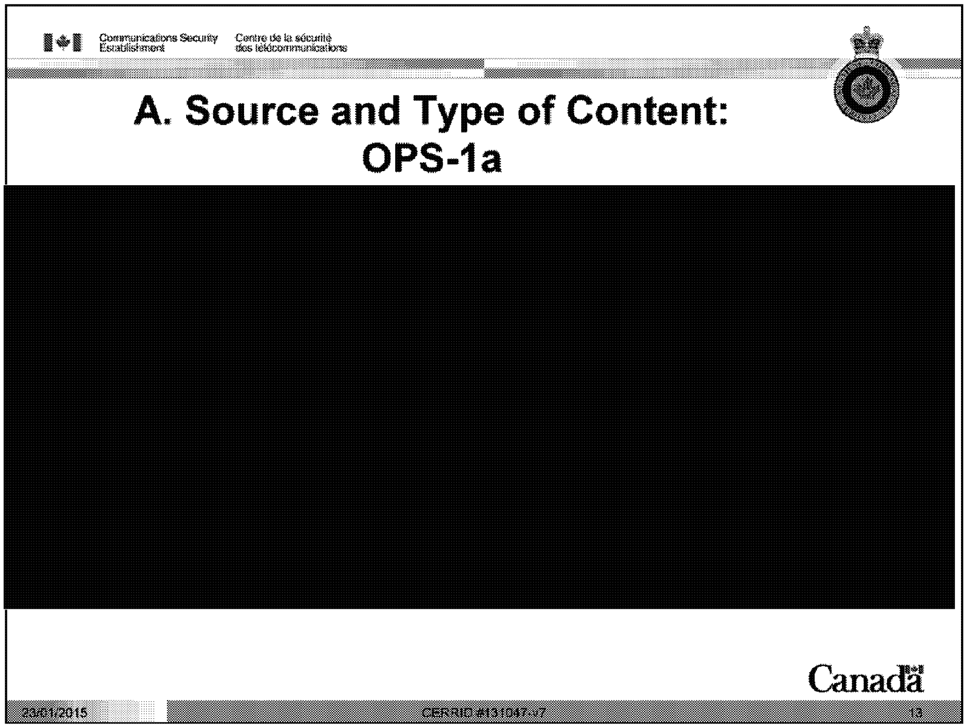
- Private communication
- Communication of a Canadian outside Canada, or
- Information about Canadians

Canada

23/01/2015 CERRID #131047-v7 12

- This brings us to the COMINT Product Release Form.
- Canadian reports with a Canadian privacy angle require sign-off by a senior managers.
- The approval authority for reports with a Canadian angle is determined by the source of the traffic on which the report is based and the type of content it contains.
- When used properly, the report release form will tell you who needs to approve your report.
- The decision to include this step was made by the Chief. It is another measure we use to safeguard the privacy of Canadians in the conduct of our activities.

- Here are a few examples of typical release forms …



Communications Security Establishment Centre de la sécurité des télécommunications

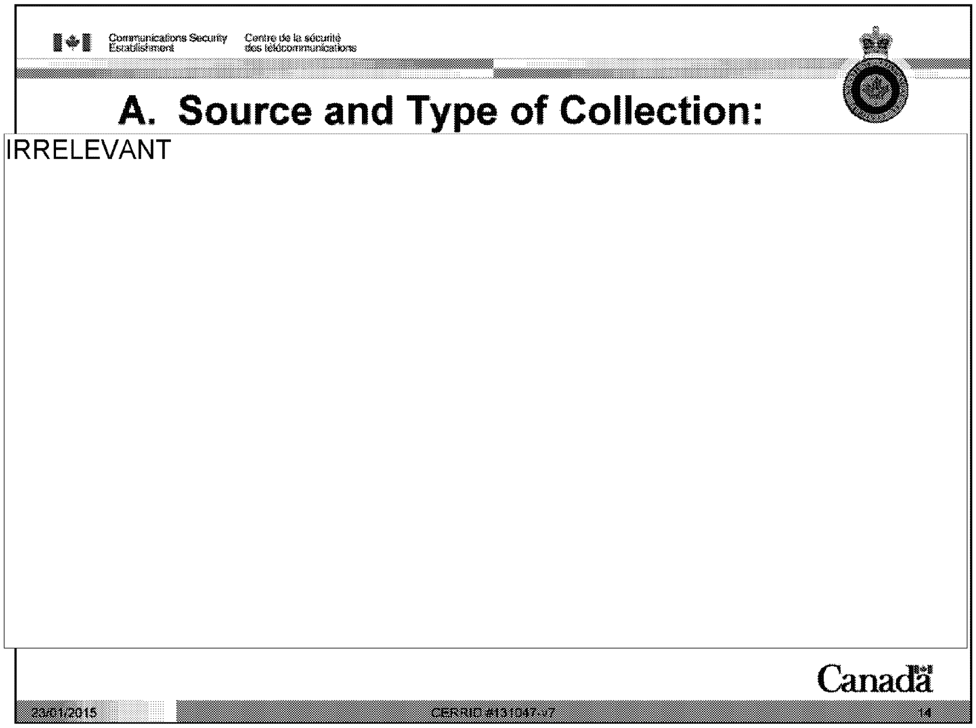
A. Source and Type of Content: OPS-1a

[redacted]

Canada

23/01/2015 CERRID #131047-v7 13

[redacted]



Communications Security Establishment   Centre de la sécurité des télécommunications

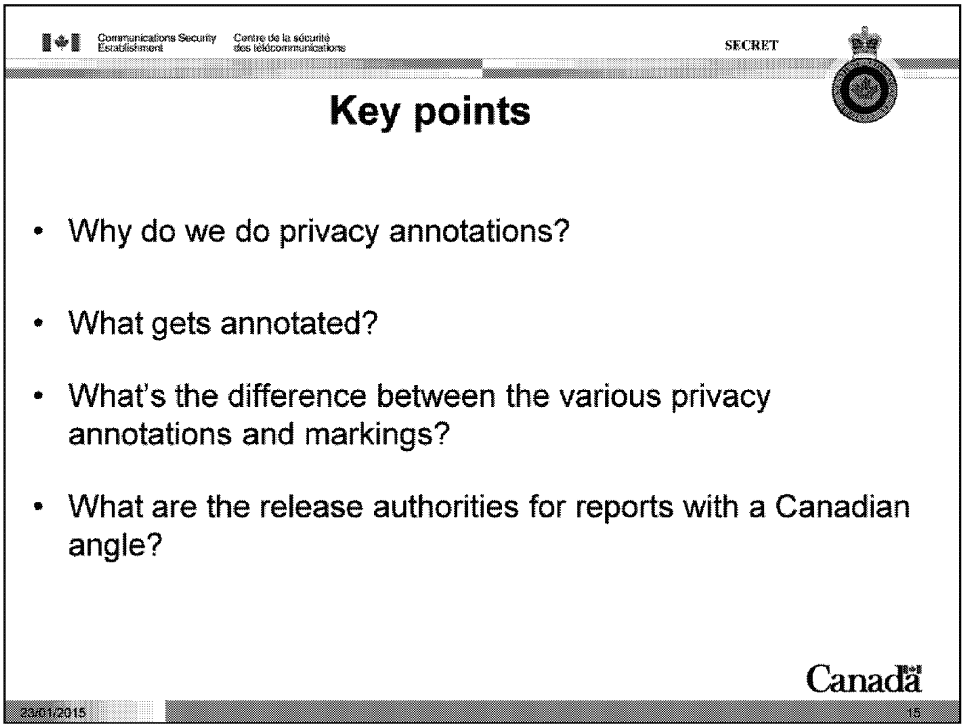
A. Source and Type of Collection:

IRRELEVANT

Canada

23/01/2015   CERRID #131047-v7   14

IRRELEVANT



Communications Security Establishment Centre de la sécurité des télécommunications

SECRET

Key points

- Why do we do privacy annotations?
- What gets annotated?
- What's the difference between the various privacy annotations and markings?
- What are the release authorities for reports with a Canadian angle?

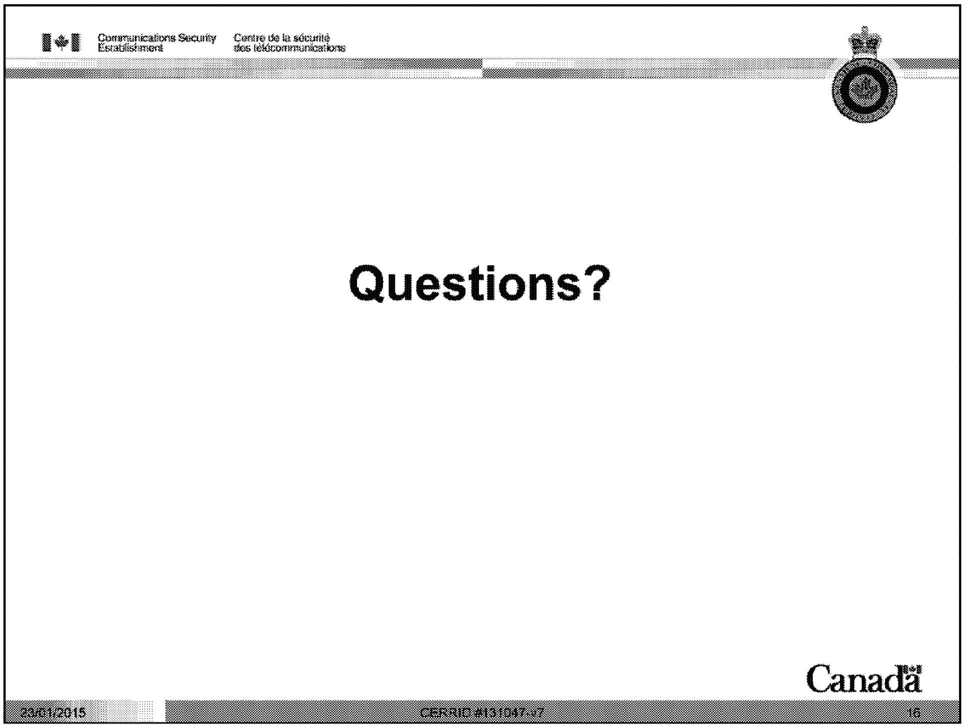
Canada

23/01/2015 15

- Our intent is to help you understand why you are obliged to make privacy annotations and markings.

- I will be covering a lot of material this afternoon. You don't need to remember it all – the key is to remember the concepts. We've also developed tools to help you determine how to annotate the traffic.
  - Ultimately, if you understand why the rules are there, you are better able to apply them appropriately.

- Please feel free to ask questions as we go along. I'll also have some time at the end to answer any questions.



Questions?

Canada