PROTECTING **CANADIAN IDENTIFYING INFORMATION** IN CSE'S FOREIGN INTELLIGENCE MANDATE

WHAT IS CANADIAN IDENTIFYING INFORMATION (CII)?

CII is information that relates to a Canadian or could be used—on its own or with other information—to identify a Canadian, like a full or partial personal name, email address, phone number, passport number, IP address, among other data elements.

DOES CSE SEEK INFORMATION ABOUT CANADIANS?

No. Under the *CSE Act*, CSE cannot direct its activities at Canadians anywhere or at anyone in Canada.

DOES CSE EVER ACQUIRE INFORMATION ABOUT CANADIANS?

Not very often. But when targeting the communications of foreign entities outside Canada, CSE sometimes incidentally acquires information about Canadians. The *CSE Act* clearly recognizes the possibility of incidentally acquired Canadian information as a result of CSE's mandated activities.

WHAT DOES CSE DO WHEN INFORMATION ABOUT CANADIANS HAS BEEN INCIDENTALLY COLLECTED?

If there is no intelligence value in the collection that contains Canadian information, the intercept is deleted from CSE's systems. However, if the Canadian information forms an essential part of the foreign intelligence — for example, the role of a named Canadian in activities that would raise national security concerns—oblique references (e.g. "Canadian 1") in a foreign intelligence report to replace specific details that might be used to identify the Canadian. This is called a "suppressed" identity. Suppressing identities in reporting is part of a suite of measures in place to help protect the privacy interests of Canadians.

WHO CAN READ CSE FOREIGN INTELLIGENCE REPORTS THAT CONTAIN SUPPRESSED CANADIAN INFORMATION?

CSE's foreign intelligence reporting is among the most safeguarded information in Canada. Specific security-cleared and indoctrinated government officials in departments designated by the Minister of National Defence may read CSE reporting if they also have the need to know the information. They are expected to handle the intelligence reporting according to strict guidelines, including restrictions on sharing the information more broadly.

CAN THE UNDERLYING DETAILS ASSOCIATED WITH THE SUPPRESSED CANADIAN REFERENCE EVER BE DISCLOSED? IF SO, TO WHOM, AND UNDER WHAT CIRCUMSTANCES?

In certain circumstances, yes. The requesting official must be in a department or agency formally designated by the Minister of Defence, must have the authority to access this information and must also have the need to know the information. The official must document and submit a new request for each report, confirming the authority under which the identifying information is being requested and agreeing to specific terms regarding the use and safeguarding of the information. Each request is vetted by CSE on a case-by-case basis.

CAN ANY ACTIONS BE TAKEN BASED ON THIS DISCLOSED CANADIAN INFORMATION?

No, not as part of the request to view the underlying Canadian information. The identifying information is provided to the requesting official as context to better understand the foreign intelligence in the report. Restrictions against using this information are clearly laid out as part of the disclosure process. If the requesting official wants to take an "action" based on the information in any CSE foreign intelligence report—regardless of whether it contains suppressed CII—a subsequent process must be used, requiring different information, vetting against different criteria and subject to different restrictions. Each "action" request is considered carefully by CSE policy experts on a case-by-case basis.

HOW DOES CSE ENSURE THE PROPER RIGOUR IS APPLIED TO THE CII DISCLOSURE PROCESS?

The *CSE Act* is clear about CSE's responsibility to apply measures to protect the privacy of Canadians, and these responsibilities are further articulated in Ministerial Authorizations and Ministerial Orders issued under the *CSE Act*. Over decades, CSE has developed a suite of measures to meet these expectations. These measures include (but are not limited to) robust legal and policy training; mandatory annual privacy tests for access to operational systems; detailed reference materials, such as policies and procedures related to handling Canadian information, as well as on-site legal and policy experts for consultation; technical measures such as data tagging and auto-deletion and strictly enforced retention periods; escalating approvals for intelligence reporting containing suppressed CII; and management oversight and compliance spot checks, among other activities that support specific CII disclosure processes.

HOW IS CSE HELD ACCOUNTABLE TO THE PUBLIC FOR PROTECTING CANADIAN PRIVACY?

In addition to Ministerial and internal managerial oversight, CSE activities related to the disclosure of Canadian identifying information have been reviewed every year for the past decade by independent review bodies, both the Office of the CSE Commissioner and the National Security and Intelligence Review Agency. CSE is also subject to review by the Offices of the Privacy and Information Commissioners, among other Officers of Parliament, all of whom report publicly on their findings. CSE has accepted all recommendations aimed at improving information management and processes for protecting privacy.

CAT. D96-38/2021E-PDF
ISBN 978-0-660-39098-7

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada