Court File No. T-2210-14

**FEDERAL COURT**

**BETWEEN:**

**THE BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION**

**Plaintiff**

**and**

**THE ATTORNEY GENERAL OF CANADA**

**Defendant**

# STATEMENT OF DEFENCE

1. The defendant admits the allegations contained in paragraphs 3, 11, 12, 17, 19, 27, 28 of the statement of claim. The facts alleged in paragraphs 4 – 10 of the statement of claim are admitted only to the extent that they are the definitions used by the plaintiff for the purpose of this civil claim. The defendant admits paragraph 1 only to the extent that it sets out the remedies sought by the plaintiff.

2. The defendant denies the allegations contained in paragraphs 13 - 16, 18, 20 - 26, 29, and 30 of the statement of claim.

3. The defendant has no knowledge of the allegations contained in paragraph 2 of the statement of claim.

**Purpose and Mandate of CSE**

4. The Communications Security Establishment (CSE) is one of Canada's key security and intelligence organizations, with a tailored three-part mandate. CSE only

carries out activities within its legislated mandate. CSE's mandate is defined in s.273.64 of the *National Defence Act*, which authorizes CSE to do three things:

> (a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities (the Foreign Signals Intelligence Mandate);
>
> (b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada (the IT Security Mandate); and
>
> (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.

5. Adopted by Parliament, following terrorist attacks on the United States on September 11, 2001, the *Anti-terrorism Act* included amendments to the *National Defence Act* adding provisions in Part V.1 continuing the existence of CSE and providing it with a legislative mandate, including specific authorities as well as prohibitions and limitations. In November, 2011, CSE became a department under Schedule I.1 of the *Financial Administration Act*. The Chief of CSE, under the direction of the Minister of National Defence (the Minister), has the management and control of CSE and all matters relating to it.

6. For the purposes of CSE's Foreign Signals Intelligence Mandate, s.273.61 of the *National Defence Act* includes the defined terms:

> (a) "global information infrastructure" includes electromagnetic emissions, communications systems, information technology systems and networks, and

any data or technical information carried on, contained in or relating to those emissions, systems or networks; and

(b) "foreign intelligence" means information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security.

7. Section 273.66 of the *National Defence Act* provides that CSE may only undertake activities that are within its mandate. In carrying out its Foreign Signals Intelligence Mandate and the IT Security Mandate, CSE's activities cannot be directed at Canadians or any person in Canada. "Canadian" is defined in s.273.61 of the *National Defence Act* as a Canadian citizen, a permanent resident within the meaning of subsection 2(1) of the *Immigration and Refugee Protection Act* or a body corporate incorporated and continued under the laws of Canada or a province. The use or retention of information acquired by CSE through the exercise of its Foreign Intelligence Mandate or its IT Security Mandate must also be subject to measures to protect the privacy of Canadians.

**Ministerial Authorizations**

8. Despite the fact that CSE is directing its activities at non-Canadians outside Canada, in relation to the Foreign Signals Intelligence Mandate, the complexity of the global information infrastructure is such that it is not possible for CSE to know ahead of time if a foreign target will communicate with a Canadian or person in Canada, or convey information about a Canadian. CSE's activities under its IT Security Mandate are directed at the acquisition of data, irrespective of its origin, that would potentially risk harm to the network being protected. As a result, the *National Defence Act* recognizes that despite CSE not directing its activities under the Foreign Signals Intelligence Mandate or the IT Security Mandate at Canadians or persons in Canada, there may be circumstances in which incidental interception of private communications or information about Canadians will occur.

9. The definition of "private communication" set out in s.183 of the *Criminal Code* and incorporated by reference in s.273.61 of the *National Defence Act* is: any oral communication, or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it, and includes any radio-based telephone communication that is treated electronically or otherwise for the purpose of preventing intelligible reception by any person other than the person intended by the originator to receive it.

10. Where CSE is carrying out its Foreign Signals Intelligence Mandate, or IT Security Mandate, the Minister may issue Ministerial authorizations in certain circumstances and subject to the Minister being satisfied that specific conditions have been met, to authorize CSE to engage in an activity or class of activities that risks incidentally intercepting private communications.

11. Ministerial authorizations relate to a specific method of acquiring foreign signals intelligence or of protecting computer systems (i.e., an activity or class of activities specified in the Ministerial authorizations). Ministerial authorizations do not relate to a specific individual or entity.

12. Where there is a Ministerial authorization applicable to a given activity, that activity is conducted in a manner consistent with the Ministerial authorization as well as the legislative requirements set out in the *National Defence Act*.

13. Where CSE activities under its Foreign Signals Intelligence Mandate risk the incidental interception of private communications, the Minister issues an authorization under s.273.65(1) of the *National Defence Act* for the sole purpose of obtaining foreign intelligence only when the Minister is satisfied that:

(a) the interception will be directed at foreign entities located outside Canada;

(b) the information to be obtained could not reasonably be obtained by other means;

(c) the expected foreign intelligence value of the information that would be derived from the interception justifies it; and

(d) satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.

14. Where CSE activities under its IT Security Mandate risk incidentally intercepting private communications, the Minister issues an authorization under s.273.65(3) of the *National Defence Ac*t for the sole purpose of protecting the computer systems or networks of the Government of Canada from mischief, unauthorized use or interference, in the circumstances specified in paragraph 184(2)(c) of the *Criminal Code* only when the Minister is satisfied that:

(a) the interception is necessary to identify, isolate or prevent harm to Government of Canada computer systems or networks;

(b) the information to be obtained could not reasonably be obtained by other means;

(c) the consent of persons whose private communications may be intercepted cannot reasonably be obtained;

(d) satisfactory measures are in place to ensure that only information that is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks will be used or retained; and

(e) satisfactory measures are in place to protect the privacy of Canadians in the use or retention of that information.

15. There are currently four active Ministerial authorizations which were issued by the Minister in 2013. Three of the active Ministerial authorizations were issued under s.273.65(1) of the *National Defence Act*. One active Ministerial authorization was issued under s.273.65(3) of the *National Defence Act*.

16. Section 273.68 of the *National Defence Act* provides that: an authorization is valid for the period specified in it, and may be renewed for any period specified in the renewal; no authorization or renewal may be for a period longer than one year; and an authorization may be varied or cancelled in writing at any time.

17. In further answer to paragraph 26 of the statement of claim, the Minister issued 78 authorizations between 2002 and 2012. These Ministerial authorizations were valid for varying periods of up to twelve months, and all have expired. Many of the 78 Ministerial authorizations covered the same class of activities over different time periods. No Ministerial authorizations were renewed beyond their original effective period.

18. All Ministerial authorizations issued under s.273.65 have contained conditions that the Minister considers advisable to protect the privacy of Canadians, including additional measures to restrict the use and retention of, the access to, and the form and manner of disclosure of, information derived from private communications.

19. It is not possible for CSE to completely avoid the interception of private communications. There were six Ministerial authorizations issued under s.273.65(1) of the *National Defence Act* in 2011. For the twelve month period that five of those Ministerial authorizations were in place none of the information intercepted was recognized as a private communications. For the remaining Ministerial authorization, the number of intercepted communications recognized as private communications that were used or retained by CSE was small.

**The Importance of Ministerial Authorizations**

20. CSE operates in a technologically complex, interconnected and rapidly evolving global electronic environment in which the volume and complexity of electronic communications is growing quickly. In conducting activities under its Foreign Intelligence Mandate, CSE has no knowledge of who a targeted foreign individual or entity outside Canada will be communicating with, nor of the location of that other communicant. It is possible that a person in Canada may be the other party to a targeted communication.

21. CSE also operates in an environment in which it must protect its methods and activities as much as possible from disclosure. Otherwise, its operations will become ineffective against foreign intelligence targets, since they will quickly learn how to evade detection.

22. Ministerial authorizations permit CSE to carry out its activities while protecting those activities from disclosure, and still protecting the privacy of Canadians.

23. CSE's ability to acquire Metadata, as well as its ability to carry out activities under its Foreign Signals Intelligence Mandate which risk the incidental interception of private communications has contributed to the prevention of attacks against Canadians and Canadian Armed Forces members, both in Canada and abroad, has assisted in facilitating the resolution of the kidnapping of Canadians abroad, has

facilitated the detection and prevention of foreign cyber threats, and has provided vital foreign affairs information which has informed and guided important Canadian government decision and actions.

24. Each year there are thousands of cyber threat incidents on Government of Canada computer systems and networks that risk compromising those systems, which may in turn compromise the private information of Canadians stored on those systems.

25. These cyber threats are characterized by rapidly increasing frequency, complexity, and scale. Wireless and anonymous connectivity to the global network is becoming increasingly common. Some of the techniques that may be used to infiltrate Government of Canada systems include unauthorized access or disclosure, malware (e.g. spyware, Trojans, worms, viruses), denial of service attacks, hijacking of computers (e.g. botnet), attempting to gain access to a computer system using a false identity (i.e., spoofing), trying to obtain personal information by pretending to be a familiar person/entity to the victim (i.e., phishing), unauthorized modification of or tampering with data, identity theft, and threats from insiders. Commercially available means to detect malicious activities are insufficient to counter these threats.

26. CSE's ability to acquire Metadata, as well as its ability to carry out other activities under its IT Security Mandate in a manner which may risk intercepting private communications on those systems and networks, allows CSE to effectively identify and address cyber threats.

**Ministerial Directive on Metadata**

27. As provided for in s.273.62 of the *National Defence Act*, the Minister has issued written directions (Ministerial directives) to the Chief of CSE with respect to certain issues or activities. Ministerial directives do not grant any authority that does not already exist in law and cannot enhance any existing authority. They serve as additional direction or guidance, setting out the Minister's expectations for, or

imposing restrictions on, CSE. Where a Ministerial directive applies, CSE's activities must be consistent with that Ministerial directive.

28. For the purposes of the directives described in paragraphs 8 and 28-30 of the statement of claim, "Metadata" means 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 or part of information which could reveal the purport of a telecommunication, or the whole or part of its content. Any reference to Metadata in this defence will be to this definition.

29. In response to paragraph 28 of the statement of claim, while two Ministerial directives have been issued in relation to Metadata, the 2011 Ministerial directive on the Collection and Use of Metadata (the Metadata Directive) supersedes and replaces the 2005 directive and is the only directive relating to Metadata currently in place.

30. The acquisition and use of Metadata is critical to the fulfillment of CSE's mandate. Metadata is important in allowing CSE to: understand how telecommunications networks operate; distinguish foreign communications from private communications so that CSE can tailor its activities to its mandate while minimizing impact on the privacy of Canadians and persons in Canada; identify malicious foreign cyber activity; and better understand and discover foreign targets. Metadata allows CSE, usually through automated tools, to filter information found on the global information infrastructure without looking at the content of any communications.

31. CSE acquires and analyses Metadata pursuant to its mandate as set out in the *National Defence Act* and subject to all of the restrictions of the *National Defence Act*, including the restrictions on directing activities at Canadians or any person in Canada and the requirement to have measures in place to protect the privacy of

Canadians. Any Metadata-related activities are also subject to applicable Ministerial directives, applicable Ministerial authorizations, and various other policies and procedures put in place to provide comprehensive protection for the privacy of Canadians and persons in Canada.

**Protection of Privacy**

32. Any personal information that CSE acquires under its mandates may only be used in compliance with the *Privacy Act*.

33. In addition to CSE's own policies and procedures to protect privacy, and the requirements set out in Ministerial authorizations and other Ministerial directives, the Minister has issued a specific Ministerial directive on the Privacy of Canadians. Pursuant to that directive, CSE may only retain and report information on or about Canadians or Canadian organizations acquired in the course of its Foreign Signals Intelligence Mandate activities in very limited circumstances.

34. Ministerial authorizations related to activities under CSE's IT Security Mandate only apply to communications to or from a computer system or network of a federal government institution. CSE does not conduct such activities on private computer systems or networks under these Ministerial authorizations. CSE only analyzes those communications that it identifies as posing potential harm to the computer system or network and only uses or retains information that is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks.

35. The Ministerial directive on the Privacy of Canadians also provides that all information obtained by CSE under its IT Security Mandate activities will be handled in a manner consistent with the *Privacy Act*.

**Sharing of Information**

36. CSE's legislated mandate involves acquiring foreign intelligence in accordance with Government of Canada intelligence priorities, and helping protect the electronic information and information infrastructures of importance to the Government of Canada. CSE shares with other government departments, for the purposes described in s. 273.64, relevant information that it gathers. CSE has extensive policies and procedures governing its information-sharing practices, which include privacy safeguards with respect to private communications, Metadata, communications of Canadians abroad and information about Canadians, in accordance with Canadian law.

37. CSE has intelligence relationships, dating back to the Second World War, with its counterpart agencies in the United Kingdom, the United States, Australia and New Zealand (the Five Eyes). CSE's precursor was created following the Second World War in order for Canada to continue to benefit from its collaboration in foreign signals intelligence collection activity with the Five Eyes. CSE shares foreign intelligence and cyber threat information with the Five Eyes to the extent authorized under the *National Defence Act*, and in accordance with Canadian national interests. The sharing of such information is further governed by international agreements, as well as domestic laws, policies and procedures, which include privacy safeguards with respect to private communications, Metadata, communications of Canadians abroad and information about Canadians.

**The CSE Commissioner**

38. In answer to paragraphs 22 and 23 of the statement of claim, it is the CSE Commissioner, and not the Office of the CSE Commissioner, who is responsible for the duties and reporting described. The Office of the CSE Commissioner supports the Commissioner in the execution and fulfillment of his duties.

39. While the CSE Commissioner provides reports to the Minister, the Office of the CSE Commissioner is not part of the Department of National Defence. The CSE Commissioner is appointed by the Governor in Council to hold office during good behaviour, for a term of not more than five years. Since April 2008, the Office of the CSE Commissioner has had its own appropriation.

40. The CSE Commissioner must be a supernumerary judge or a retired judge of a superior court. Former Commissioners have included a retired Chief Justice and two retired Justices of the Supreme Court of Canada, a retired Chief Justice of the Quebec Court of Appeal and a retired Justice of the Federal Court of Appeal. The current Commissioner is a supernumerary judge of the Court Martial Appeal Court of Canada and former judge of the Superior Court of Quebec.

41. Pursuant to his legislative mandate, the CSE Commissioner provides a robust review of the activities of CSE to ensure that they are in compliance with the law. The CSE Commissioner is required by law to inform the Minister and the Attorney General of Canada of any action by CSE which the CSE Commissioner believes may not comply with the law, including the *National Defence Act*, the *Canadian Charter of Rights and Freedoms*, the *Privacy Act* and the *Criminal Code*. Furthermore, the Minister is required to table the CSE Commissioner's annual report in Parliament. The CSE Commissioner has never identified any actions of CSE as unlawful. The CSE Commissioner has recognised in his reviews that CSE conducts all of its work in a culture of respect for the law and for the privacy of Canadians.

42. CSE Commissioners have recommended legislative amendments intended to clarify certain ambiguities, for example in s.273.65 of the *National Defence Act*. However, contrary to the plaintiff's allegation in paragraph 25, the first reference to proposed statutory amendment to the *National Defence Act* in the annual report of the CSE Commissioner appeared in the 2005-2006 annual report.

43. As part of the reviews conducted, the CSE Commissioner has considered the number of private communications intercepted and has verified how CSE treated and used these communications. This has involved examining, for compliance with the law, a sample of the CSE Commissioner's choosing of any private communications intercepted, used or retained. For the period 2012-2013, at the end of the reporting period staff from the Office of the CSE Commissioner reviewed all of the private communications that CSE used and retained under its Foreign Signals Intelligence Ministerial Authorization.

44. The CSE Commissioner has all the powers of a commissioner under Part II of the *Inquiries Act*, including the power to summon witnesses to give evidence under oath or solemn affirmation. In exercising his duties, the Commissioner regularly reviews CSE's operational activities, examines CSE's policies, Ministerial directives, and procedures. The CSE Commissioner, and the staff of the Office of the CSE Commissioner, have access to CSE's premises, documents, files and personnel. Reviews of CSE activities also include extensive testing, sampling, first-hand observations, and interviews with CSE personnel and other officials from federal government departments and agencies.

45. In addition, all active Ministerial authorizations issued under s.273.65 of the *National Defence Act* specifically require CSE to support and assist the Commissioner in reviewing the activities carried out under the Ministerial authorization. CSE provides briefs and demonstrations of activities as well as written responses to written inquiries posed through the Commissioner's office.

46. The Commissioner submits a detailed classified report to the Minister for each review of CSE's activities. Since 1996, the Commissioner has submitted approximately 81 classified reports to the Minister covering reviews of the full scope of CSE activities including, inter alia:

(a) CSE's efforts to protect the privacy of Canadians;

(b) CSE's foreign signals intelligence collection activities under Ministerial authorizations;

(c) CSE information technology security activities under Ministerial authorizations;

(d) CSE activities in support of specific law enforcement agencies;

(e) CSE's counter-terrorism activities;

(f) CSE's acquisition and implementation of technologies as a means to protect the privacy of Canadians;

(g) Annual reviews since 2009 of CSE's disclosures of Canadian identity information to Government of Canada clients;

(h) CSE's retention and disposal of intercepted or copied communications; and

(i) CSE's metadata activities.

47. Past recommendations for improvements to CSE processes have covered policy issues, technical and operational practices, and appropriate accountability structures. When warranted by findings, the CSE Commissioner has made recommendations regarding ways in which CSE can further improve its privacy protections. As a result of such recommendations, CSE has created new and changed existing policies and procedures to further strengthen privacy protections.

48. CSE has been, and continues to be, subject to review by the Privacy Commissioner and audit by the Auditor General.

**Practices in Comparable Jurisdictions**

49. Other comparable jurisdictions, including members of the Five Eyes, also utilize executive authorization regimes to authorize the interception of private communications incidental to collecting foreign intelligence or conducting IT security activities.

**Jurisdiction and Mootness**

50. In response to paragraphs 1(b), (c), (e), and (f) of the statement of claim, ss.18(1) and (3) of the *Federal Courts Act* gives the Federal Court exclusive jurisdiction to grant declaratory relief against any Federal board, commission or other tribunal and to hear and determine an application for declaratory relief against any federal board, commission or other tribunal only by way of an application for judicial review made under section 18.1 of the *Federal Courts Act*.

51. The question of whether any Ministerial authorization which is no longer in effect infringes the *Charter* is moot and ought not to be considered by this Court. Similarly, the 2005 Ministerial directive on the Collection and Use of Metadata is no longer in effect and the question of whether it infringes the *Charter* is moot and ought not to be considered by this Court.

***Charter,* Section 2(b)**

52. The impugned provisions do not interfere with freedom of expression in either purpose or effect and therefore do not infringe s.2(b) of the *Charter*. In particular, Metadata is not a communication that conveys or attempts to convey meaning, but rather information of a technical nature generated through the act of communicating, so any acquisition or use thereof by CSE cannot interfere with freedom of expression. Should any indirect interference with freedom of expression be found, it is in any case more appropriately dealt with under the s.8 privacy-related analysis.

***Charter,* Section 8**

53. The impugned provisions also do not violate s.8 of the *Charter*.

54. In relation to Metadata, when Metadata acquired and used by CSE is the subject of a reasonable expectation of privacy, the acquisition of that Metadata is authorized by the *National Defence Act* and CSE has privacy safeguards in place. Certain of the Metadata acquired and used by CSE is not subject to a reasonable expectation of privacy.

55. Any interference with information in which a Canadian or person in Canada has a s.8-protected reasonable expectation of privacy which may occur as a result of the impugned provisions is reasonable because any such interference is carried out in the context of foreign intelligence and IT security activities (not law enforcement) and is:

(a) authorized by the *National Defence Act* and, where applicable, through the Ministerial authorizations provided for in the *National Defence Act*;

(b) in furtherance of government objectives of the utmost importance; and

(c) minimally intrusive in terms of the type of private information which may be acquired from telecommunications or their Metadata, as well as tailored in scope to the objectives of Part V.1 of the *National Defence Act* and minimized as much as possible through a variety of privacy safeguards provided for in the *National Defence Act*, Ministerial directives, Ministerial authorizations and other applicable policies and procedures.

56. In addition, CSE's activities are regularly and thoroughly reviewed by an independent entity, the CSE Commissioner, to ensure that CSE complies with the applicable laws, Ministerial directives, Ministerial authorizations and policies. The

CSE Commissioner specifically examines and reports on whether satisfactory measures are in place to protect the privacy of Canadians.

***Charter,* Section 1**

57. In the alternative, if there is any infringement of either ss.2(b) or s.8 of the *Charter*, such infringement is justified under s.1. in particular, Canada is addressing several pressing and substantial objectives, including facilitating the protection of Canadians against threats such as terrorism, foreign kidnapping, and attacks on Canadian Armed Forces members and other personnel abroad, the detection and prevention of cyber threats, the protection of vital Canadian government electronic information and information infrastructures and the provision of foreign intelligence to guide important Canadian government decisions and actions. In addition, the *National Defence Act* establishes a system of authorization and review which allows for the protection of CSE's methods from public disclosure in order to ensure their ongoing effectiveness in pursuit of CSE's mandates.

58. In today's globalized and networked environment, acquiring and using foreign signals intelligence and providing advice, guidance and services to help protect against threats to the integrity and security of electronic information and information infrastructures of importance, which carry with them an unavoidable risk of incidental interception of private communications, are rationally connected to the Government of Canada's need to protect its international affairs, defence and security interests and important electronic information and information infrastructures.

59. The Government's objectives are achieved in a manner which minimally impairs any *Charter* protected rights affected. CSE is required to conduct its activities in a tailored, but technologically and practically feasible manner, subject to executive oversight and independent review, while also imposing safeguards in relation to any

Canadian privacy interests which might be incidentally impacted through CSE's activities.

60. The beneficial effects of allowing CSE to carry out activities necessary to protect Canada's national security, foreign affairs and national defence as well as to protect the Government's electronic infrastructure, are significant and far outweigh any minimal interference with either freedom of expression or privacy which may incidentally occur.

**Response to Relief Sought**

61. The defendant opposes the granting of the relief sought in paragraph 1 of the statement of claim.

62. The defendant seeks an order dismissing this proceeding, with costs.

63. In the alternative, in the event that any part of the impugned laws is found to unjustifiably infringe a *Charter* right, the defendant says that any declaration of invalidity should be suspended for one year to allow Parliament sufficient time to amend the current legislation as appropriate.

DATE: November 26, 2014

William F. Pentney
Deputy Attorney General of Canada
Per: Donnaree Nygard
Department of Justice
B.C. Regional Office
900-840 Howe Street
Vancouver, British Columbia
V6Z 2S9
Tel: (604) 666-3049
Fax: (604) 775-5942
File: 4387019

Solicitor for the Defendant

TO: B.C. Civil Liberties Association

Joseph J. Arvay, Q.C.
Farris, Vaughan Wills & Murphy LLP
P.O. Box 10026, Pacific Centre South
25th Floor, 700 West Georgia Street
Vancouver, British Columbia
V7Y 1B3

Tel: (604) 684-9151
Fax: (604) 661-9349

David J. Martin
Martin & Associates
863 Hamilton street
Vancouver, British Columbia
V6B 2R7

Tel: (604) 682-4200
Fax: (604) 682-4209

Solicitors for the Plaintiff