



Public Inquiry Into Foreign Interference in Federal
Electoral Processes and Democratic Institutions

Enquête publique sur l'ingérence étrangère dans les
processus électoraux et les institutions démocratiques
fédéraux

Public Hearing

Audience publique

**Commissioner / Commissaire
The Honourable / L'honorable
Marie-Josée Hogue**

VOLUME 3

Held at :

Library and Archives Canada
Bambrick Room
395 Wellington Street
Ottawa, Ontario
K1A 0N4

Wednesday, January 31, 2024

Tenue à:

Bibliothèque et Archives Canada
Salle Bambrick
395, rue Wellington
Ottawa, Ontario
K1A 0N4

Le mercredi 31 janvier 2024

INTERNATIONAL REPORTING INC.

<https://www.transcription.tc/>

(800)899-0006

II Appearances / Comparutions

Commission Lead Counsel / Procureure en chef de la commission	Shantona Chaudhury
Commission Counsel / Avocat(e)s de la commission	Gordon Cameron Erin Dann Matthew Ferguson Hubert Forget Howard Krongold Hannah Lazare Jean-Philippe Mackay Kate McGrann Lynda Morgan Siobhan Morris Annie-Claude Poirier Gabriel Poliquin Natalia Rodriguez Guillaume Rondeau Nicolas Saint-Amour Daniel Sheppard Maia Tsurumi
Commission Research Council / Conseil de la recherche de la commission	Geneviève Cartier Nomi Claire Lazar Lori Turnbull Leah West
Commission Senior Policy Advisors / Conseillers principaux en politiques de la commission	Paul Cavalluzzo Danielle Côté
Commission Staff / Personnel de la commission	Annie Desgagné Casper Donovan Michael Tansey

III

Appearances / Comparutions

Ukrainian Canadian Congress	Donald Bayne Jon Doody
Government of Canada	Gregory Tzemenakis Barney Brucker
Office of the Commissioner of Canada Elections	Christina Maheux Luc Boucher
Human Rights Coalition	Hannah Taylor Sarah Teich
Russian Canadian Democratic Alliance	Mark Power Guillaume Sirois
Michael Chan	John Chapman Andy Chan
Han Dong	Mark Polley Emily Young Jeffrey Wang
Michael Chong	Gib van Ert Fraser Harland
Jenny Kwan	Sujit Choudhry Mani Kakkar
Media Coalition	Christian Leblanc Patricia Hénault
Centre for Free Expression	John Mather Michael Robson

IV Appearances / Comparutions

Churchill Society	Malliha Wilson
The Pillar Society	Daniel Stanton
Democracy Watch	Wade Poziomka Nick Papageorge
Canada's NDP	No one appearing
Conservative Party of Canada	Michael Wilson Nando de Luca
Chinese Canadian Concern Group on The Chinese Communist Party's Human Rights Violations	Neil Chantler
Erin O'Toole	Thomas W. Jarmyn Preston Lim
Senator Yuen Pau Woo	Yuen Pau Woo

V
Table of Content / Table des matières

	PAGE
Introduction of the Expert Panel by/Introduction du panel de spécialistes par Mr. Gordon Cameron	1
Presentation by /Présentation par Mr. Alan Jones	3
Presentation by /Présentation par Mr. John Forster	13
Presentation by/Présentation par Mr. Richard Fadden	17
Questions to the panel by/Questions aux panélistes par Mr. Gordon Cameron	26

Ottawa, Ontario

--- L'audience débute le mercredi 31 janvier 2024 à 10 heures

The hearing begins January 31, 2024 at 10:00 a.m.

THE REGISTRAR: Order, please. À l'ordre, s'il vous plait.

This sitting of the Foreign Interference Commission is now in session. Commissioner Hogue is presiding.

Cette séance de la Commission sur l'ingérence étrangère est maintenant en cours. La commissaire Hogue préside.

The time is 10 o'clock. Il est 10 heures.

COMMISSIONER HOGUE: So good morning, everyone. Alors, bonjour.

MR. GORDON CAMERON: Bonjour.

COMMISSAIRE HOGUE: Première chose, les participants en ont été informés hier soir, mais simplement pour que le public soit au courant, des contraintes au niveau des panélistes font en sorte qu'aujourd'hui exceptionnellement le panel terminera autour de midi 30 ainsi que la journée d'audience.

Alors, ceux qui veulent vaquer à d'autres occupations cet après-midi sont évidemment les bienvenus.

Mr. Cameron, if you want to come to the podium. I understand it's you that will lead the panel this morning, so.

--- INTRODUCTION OF THE EXPERT PANEL BY/INTRODUCTION DU PANEL DE SPÉCIALISTES PAR MR. GORDON CAMERON:

1 **MR. GORDON CAMERON:** Thank you, Madam
2 Commissioner.

3 My name is Gordon Cameron. I'm one of the
4 Commission counsel. Today we have a panel of three former
5 national security intelligence public officials. The parties
6 might have had a chance to read their biographies, but I'll
7 do a brief introduction of them.

8 Seated closest to the counsel tables is Mr.
9 Richard Fadden. Mr. Fadden served as Director of the
10 Canadian Security Intelligence Service from 2009 to 2013 and
11 was then the National Security Advisor to the Prime Minister
12 in 2015 and 2016. Prior to that, he held various Deputy
13 Minister positions, including the Deputy Minister of Defence
14 in the government, and currently, among other roles, he is a
15 senior Fellow at the University of Ottawa's graduate school
16 of Public and International Affairs.

17 Seated beside Mr. Fadden is Mr. Alan Jones.
18 Alan Jones began his working career with the RCMP and then
19 moved to CSIS, where he held various operational and
20 management positions, rising to Assistant Director of
21 Operations at CSIS, thus responsible for all operational
22 programs, and then as Assistant Director for Technology,
23 which included both corporate and operational technology. He
24 is currently an executive advisor in the University of
25 Ottawa's Professional Development Institute for courses on
26 national security and cyber security.

27 Mr. John Forster joins us by video link and
28 he -- Mr. Foster was the Chief of the Communications Security

1 Establishment, which is, as you might have learned from some
2 of the filed materials, the federal government's agency for
3 signals intelligence and cyber security. He was in that
4 position from 2012 to 2015. Prior to that, he, too, held
5 various Deputy Minister and Associate Deputy Minister
6 positions, including as Deputy Minister of Defence. And
7 since his retirement from the government, he has continued as
8 a consultant with CSIS with National Defence and with
9 Infrastructure and Communities.

10 Madam Commissioner, what we plan to do first
11 is to have the panelists make an opening presentation
12 expressing some of their views on the topics before us today,
13 and though there's no necessary order to this, we've decided
14 that we would begin by asking Alan Jones to begin with his
15 comments.

16 So Mr. Jones, could you get us started?

17 **--- PRESENTATION BY/PRÉSENTATION PAR MR. ALAN JONES:**

18 **MR. ALAN JONES:** Thank you very much for the
19 opportunity to speak today.

20 I thought I might start my comments with
21 making some commentary on the panels yesterday, which I found
22 very informative. I was here yesterday, and there were some
23 -- there was a discussion and some information offered that I
24 thought I would offer some comments on for context.

25 One, I thought the overview by Professor Leah
26 West on the process around section 38 was extremely useful
27 and the comparison to what happened in the Arar Commission
28 was informative and useful and a very appropriate way to

1 introduce those topics to this Commission because things will
2 probably unfold in a similar manner, although obviously
3 there's been some evolution of that process and law since
4 that.

5 I was very grateful to -- for Professor
6 West's submission on that.

7 One point that did not come out clearly I
8 thought I would make was the classified information is not
9 owned per se by the agencies. It is owned by the Crown.
10 Information is governed by federal law, by precedents, by
11 federal policy and the decisions for disclosure are made on
12 behalf of the Governor of Canada, not solely on the volition
13 of agencies for what they would or would not want to
14 disclose.

15 **MR. GORDON CAMERON:** Excuse me, Mr. Jones.
16 Could you move the microphone closer to your mouth just to
17 make sure the interpreters and people can hear you better?

18 **MR. ALAN JONES:** Is that better?

19 Okay. There was also considerable reference
20 to the Arar Commission, which I had considerable involvement
21 in. And I think the process around disclosure in Arar is
22 very relevant to this Commission, but I was a bit not
23 concerned, but I don't necessarily view -- actually, I don't
24 view at all that the focus of the Arar Commission, which was
25 on wrongdoings, is the focus of this Commission.

26 I think that there is quite a divergence in
27 the Terms of Reference for this Commission to the Arar
28 Commission and I was a little concerned that the impression

1 would be left that this focus was on wrongdoings by whoever,
2 which changes the complexion of a number of things.

3 One, it changes the complexion of requests
4 for disclosure, particularly if it's to third parties, where
5 a third party, if it's another country, is -- because other
6 countries are watching this process. This is public. That
7 another country if it is asked to disclose into a Commission
8 on wrongdoings then may take something of a defensive
9 position about what it is willing to disclose compared to a
10 request for disclosure for fact finding.

11 The other being if there is a perception of
12 wrongdoing, criminal wrongdoing, as there was in Arar, that
13 that has an effect on the type of disclosure. The
14 credibility of information, the source of information, where
15 that information comes from is looked at in a very different
16 context than it is for a fact finding.

17 So I just wanted to put -- make that as a
18 clear point that I think this Commission is not Arar 2, so to
19 speak in terms of its focus and its intent, but the analogue
20 for the process around disclosure in Arar is very relevant.

21 The other point I would make about Arar, that
22 was a -- the subject matter was totally different. It was
23 counter-terrorism as opposed to foreign interference, which
24 involves different agencies, a different methodology for how
25 that information is collected, how intelligence produced, and
26 obviously, the context of Arar was post-911, which was a
27 different time than we are in now.

28 In reference to third party intelligence, we

1 are, as the comment was made, a net importer-receiver of
2 intelligence produced by allies and partners, primarily the
3 Five Eyes, but also NATO, but also others. Government of
4 Canada has relationships with many different organizations
5 worldwide. The world is bigger than the Five Eyes in NATO,
6 and those relationships are all important.

7 But I think what is important to bear in mind
8 is those other countries run their intelligence programs not
9 for the benefit of Canada. They run their programs for the
10 benefit of protecting their own countries.

11 Intelligence that they provide to Canada is a
12 byproduct, or sometimes an intentional product if their own
13 interests are involved, of their programs which are designed
14 to protect themselves. They will disclose intelligence to
15 Canada, share intelligence with Canada for collective
16 security. They'll disclose if they believe that there is a
17 threat to their own country that is emanating from Canada or
18 from someone or an organization linked to Canada and they're
19 looking for cooperation. They will disclose as general
20 information for a broad-based threat.

21 They will disclose sometimes just to be in
22 good standing with Canada because they have other relations,
23 even economic and tourism relations, that they want to make
24 sure that Canada understands that they are safe and they are
25 working hard to keep their borders safe. But their primary
26 intent of producing intelligence is for their own purposes.

27 So when Canada makes a request for disclosure
28 and there are at risk their sources, whether they're human

1 sources, technical sources or if they're covert operators
2 working for their agencies or their methodologies, they must,
3 in their deliberations about disclosure, measure the impact
4 on their own national security when providing that
5 information to Canada or reviewing any type of disclosure
6 request for public disclosure.

7 So it is not simply that they're looking at
8 how it affects Canada. It affects them.

9 There's also an element that was discussed
10 yesterday of the time that it takes to process disclosure
11 requests and go through the section 38 process of the *Canada*
12 *Evidence Act*, that it is slow. It is not simply a Canadian
13 process.

14 When Canada makes that request to a third
15 party, to another country, that request ends up going to
16 specialized sections within those agencies which are policy
17 and legal sections who tend to be swamped with requests from
18 their own internal processes, whether they're preparing
19 documents for Congressional hearings, for Parliamentary or
20 state inquiries or responding to lawsuits or responding to
21 other countries. So it -- I think it's important to
22 understand that, although it is tempting at times to think
23 that another country is dragging its feet and doesn't want to
24 cooperate, you're entering into yet another bureaucratic
25 process with deliberations take a long time and the response
26 time is not necessarily compelled by the response time of a
27 Canadian interest. They have to look at their own priorities
28 as well.

1 And while pressure can be put to say, "Look,
2 this is very important, we need you to respond within this
3 timeframe", there's often goodwill. They often do
4 understand. Many countries want to understand, do understand
5 that this is important. They have their own pressures to
6 deal with.

7 There was a comment made about sometimes that
8 there is tension around even asking another country for
9 disclosure on certain topics. Most of the countries that
10 Canada deals with, the Five Eyes in NATO, there is -- that's
11 really not an issue.

12 They have their own processes. They
13 understand why we were asking -- we would be asking those
14 questions. They may not be happy about it because sometimes
15 they would wish that Canada would resolve its own issues
16 without asking them to have to become part of it. But that
17 there's no -- there's no real risk of damage to the
18 relationship, we'll work that through.

19 Other countries who do not have similar
20 systems to Canada, who do not have rule of law, who don't
21 have democratic governments, not liberal democracies, their
22 response to these types of questions sometimes is quite
23 different. They don't understand why they're being asked.
24 They will have -- they'll try and overlay their own lens as
25 to why we'd be asking those questions. That sometimes
26 requires a lot of finesse, a lot more work and sometimes they
27 just simply either don't respond or they say no.

28 The types of responses that you can get can

1 be a "Yes, we will disclose", "We will disclose part of what
2 you want, but not all of it", but sometimes you get a nuanced
3 response which is, "We have disclosed this to the Government
4 of Canada for you to use as you see -- as you require, but
5 we'll also hold you accountable for the consequences of your
6 disclosure".

7 This is that middle ground grey area where
8 you have to make decisions about what you disclose and you
9 don't, so it's not -- again, there's no formula for this and
10 no written rules.

11 There's very ample discussion, as I say,
12 about the need to protect human sources. Obviously, we have
13 an obligation, legal and moral, to protect people who are
14 putting their lives at risk to provide intelligence to Canada
15 to protect Canada.

16 Often they are providing intelligence to
17 Canada, particularly in the context of foreign interference,
18 because they want to protect themselves, their families,
19 their communities and others, but they are concerned that the
20 exposure of their cooperation with the government would have
21 negative consequences on them reputationally in business or
22 for more dire consequences to their family and their
23 interests back in whatever country that is the source of the
24 coercion or the intimidation or the interference.

25 These are real issues. These real street-
26 level issues that you have to deal with when you're dealing
27 with a disclosure request because these are human beings.

28 The disclosure of technical sources -- and

1 there was a comment yesterday that was made that I thought
2 was very -- was worth repeating, is in intelligence reports,
3 the source is not disclosed in reports itself. In fact, the
4 type of source is not referenced. There is no reference to
5 whether it is a human source or a technical source because
6 the mere reference as to whether it is a human or a technical
7 source can point to exactly what that source is, so the
8 source itself is anonymized in every reporting.

9 The identity of that source is always kept
10 separate in a separate process, and that is done for the
11 need-to-know principle and to protect those assets.

12 Technical assets are often a technical
13 source, has often been deployed or put in place with the
14 support of a human source, so you can't necessarily partition
15 those disclosure requests. Technical sources are often very,
16 very expensive, but they also come with their own risks, and
17 the risks are that a human source may have been in support or
18 that individuals may have been operating in covert positions
19 where there was physical risk to put that source in place.

20 Just as a bit of an anecdote, hyperbole, I
21 think most people are aware that in the CIA lobby there's a
22 memorial wall with stars on the wall. For every CIA agent
23 that has been killed, there's a star on the wall.

24 The NSA, which is CSE's equivalent, has a
25 similar memorial wall. There are more stars on the NSA wall
26 than there is on the CIA wall. So the physical risk around
27 technical sources is not trivial. It's not inconsequential.
28 It does exist for various reasons.

1 But there are risks to these. It's not
2 simply a technical source.

3 In both of those cases, whether it's a human
4 source or technical source, they've been developed, often
5 over years of time. They've been developed because there's a
6 need for them. And so if there's a loss of them, you also
7 lose the ability to produce that intelligence reporting on
8 future threats.

9 So that goes into the disclosure
10 considerations as well, is if you lose those sources for a
11 disclosure, although it may be a very important reason, how
12 do you replace them and are you leaving yourself vulnerable
13 because there is a gap?

14 Just to sum up, I've outlined a lot of things
15 of concerns based on the conversations yesterday, but I have
16 long believed that there is scope for more disclosure of the
17 good work that is done by the intelligence services in Canada
18 on behalf of the people of Canada and the Government of
19 Canada, that there are ways that we could look at being more
20 transparent, but managing to protect those sources, those
21 risks in future. I'm not sure that the current rules and
22 laws as they're interpreted now have been as innovative as
23 possibly as they could be in a modern context and that there
24 may be ways to interpret. I'm not going to go too far down
25 that road because there's legal issues in there, but I think
26 that there is a very -- at times the narrowest interpretation
27 of risk based on the various ways that disclosures can happen
28 that there may be latitude on innovation and scope for

1 broader disclosure. One of them might be -- is what I would
2 call a temporal issue, because over time, the risk to -- of
3 disclosure may be mitigated, not necessarily. But there are
4 times when a human source, for as long as they live, has to
5 be protected, or protecting the source is long. But there
6 are circumstances when a risk that may have exist to
7 disclosure of information that is a year, or two, or five
8 years old is not the same as information that is longer than
9 10 years old or even in a different timespan. And I'm not
10 sure we've ever really looked at that temporal aspect or the
11 depth that possibly we could as to what that means. That is
12 one example. But I think more work needs to be done. I
13 think it is very important for the credibility of agencies,
14 for the people of Canada and Parliamentarians to understand
15 why agencies are doing what they're doing, to understand the
16 good work that is being done on behalf of the people of
17 Canada, and the only way to do that is to be more
18 transparent. And I think -- I urge that more work be done on
19 this in future.

20 So I've laid out a bunch of risks, but at the
21 same time, I want to put that marker down as we need to do
22 better on disclosure than we have in the past.

23 **MR. GORDON CAMERON:** Okay. Thank you, Mr.
24 Jones.

25 And now, Mr. Forster, if we can hear some
26 comments from you? Let's see if the video comes up.

27 **MR. JOHN FORSTER:** Okay. Thank you, Gordon.
28 Can you hear me all right?

1 **MR. GORDON CAMERON:** Yes, that's working
2 well.

3 **--- PRESENTATION BY/PRÉSENTATION PAR MR. JOHN FORSTER:**

4 **MR. JOHN FORSTER:** Okay, great. Good morning
5 and thank you for the opportunity to be here this morning.
6 As Gordon mentioned, I worked in several departments in my
7 career, three of which involved national security and
8 defence. At Transport Canada we were consumers of
9 intelligence to try and identify threats to the
10 transportation system, particularly aviation, such as putting
11 in place a liquid ban overnight due to a flight from the UK.
12 As Chief of the Communications Security Establishment, we
13 were collectors of foreign intelligence that we provided to
14 other departments. And finally, as Deputy Minister of
15 National Defence, which has a very significant intelligence
16 function, we were both a collector and a consumer of
17 intelligence to assist the Armed Forces.

18 I'll start off by saying I'm not a lawyer and
19 I'm not a specialist in intelligence classification, but I
20 thought I'd share a few perspectives from my experience as
21 both a collector and consumer of intelligence products. And
22 I support the inquiry's view that, you know, it wishes to be
23 as transparent as possible and to make as much information
24 public as possible. In fact, there was many times,
25 especially when I was at CSE, and during many appearances in
26 front of parliamentary committees where it would have made my
27 job as the head of one of the agencies a lot easier to
28 disclose classified information, to explain threats to

1 Canada, or explain the operations of my department.

2 But even if it wasn't against the law, there
3 were real reasons that prevented me from being able to do
4 that, so I'll touch on a few of these, and Al had mentioned
5 some of them already, but I'll touch on a few of the key
6 constraints that we faced.

7 First, intelligence agencies like CSE and
8 CSIS must at all costs protect their sources, their
9 techniques, their technology. So when you publish a report
10 about a conversation, even if you take out names and you
11 redact locations and some of the specifics, you can easily
12 divulge who or how the information was obtained, and that
13 puts your sources at risk, or your target will take steps to
14 evade your technology and techniques and you go dark. And so
15 that's always going to be a very critical consideration.

16 Second, important to remember, intelligence
17 is not fact. The disinformation campaigns are escalating.
18 Attribution, particularly that's identifying the real source
19 of the information, particularly in the cyber domain where
20 CSE works, can be extremely difficult. And so as a result,
21 if you publish a report, even with varying degrees of
22 confidence, there may be a risk of inadvertently disclosing
23 information before further analysis confirms or corrects it.

24 Third, intelligence requires good analysis
25 and context. So when I began at CSE, I was cautioned about
26 consuming raw intelligence, a report of a conversation, a
27 report of a meeting, because they can be misleading. So
28 analysts combine an in-depth knowledge of their subject, the

1 trends, the context, reporting from different sources to
2 eventually build an assessment. So when you publish a single
3 individual report, it may mislead the reader who doesn't have
4 access to other critical reporting and context. This is a
5 caution I shared with previous Ministers of National Defence.

6 Now fourth, as Alan mentioned, a lot of the
7 information is not ours to share. We are a huge net importer
8 of intelligence. We rely on our allies, particularly the
9 Five Eyes, particularly in the SIGINT world, for much of it.
10 And we consume more than we produce. And so the originator
11 of the intelligence imposes their conditions or caveats on
12 how we can use it and we need their approval. And if you
13 disclose it without that approval, no matter -- and it may
14 take long time, they'll simply stop sharing with you. And
15 Canada would be severely weakened.

16 Finally, another key point I think to mention
17 is the need to know, as Alan referenced it earlier. Some of
18 the intelligence is so sensitive, the source so crucial, and
19 the information so valuable, there are only a handful of
20 people in the federal government that have access to it.
21 It's compartmentalized, it's highly restricted, and you must
22 be indoctrinated to review it in a secure location. It's not
23 routinely available even to people with a top-secret
24 clearance, and that goes for deputy ministers as well.

25 So does this mean that all intelligence needs
26 to be kept secret and can't be made public? Not at all, and
27 I think, in fact, CSIS wants to be able to share more of its
28 intelligence with governments and companies and universities,

1 but it has to require a change to its Act. And it's really
2 important that the inquiry has the access to what it needs
3 and can challenge the government on what can be released.

4 So there's three points I'll make in that
5 respect. One, I think it's important for participants and
6 the public to remember that, as I understand it, the inquiry
7 will have full access to all of the unredacted information.
8 So even if they can't release it or refer to it explicitly,
9 the inquiry certainly will be able to consider it in doing
10 its work and formulating its findings.

11 The second, the inquiry can and should
12 challenge the government to justify what can't be released
13 and why. Departments do, on occasion, over-classify
14 material. There can be a natural inclination to default to
15 less is more. So it's important that a challenge process
16 include a senior-level review of an initial decision by an
17 expert where a broader perspective may be required, but it
18 can't be in every instance. And even though the inquiry can
19 challenge it to the Justice Department or the court, it's
20 such -- so time consuming and resource intensive, both for
21 the inquiry and the government that it's -- I think a spirit
22 of cooperation will be critical and it will need to be
23 communicated by the government to -- at the senior level.

24 The third point I would make is I think it
25 will be important for the government and agencies to produce
26 unclassified versions of reports, public summaries, or an
27 unclassified assessment. You know, it's not necessary that
28 specific details, names, locations, dates, specifics of a

1 conversation necessarily be disclosed to get the gist of the
2 report and what its impacts are on the Inquiry's mandate.

3 You know, there is no simple kind of general
4 rule or one-size-fits-all solution that we'll find. Each
5 report will require careful consideration. There are real
6 risks at stake. And public interest and transparency will be
7 -- is very important, but it must be balanced also against
8 very real and serious national security interests, which are
9 also in the public interest.

10 So I think the public date the Inquiry is
11 hosting this week is really an important and very valuable
12 one, and I'll conclude there and turn it back to Gordon.

13 **COMMISSIONER HOGUE:** Thank you.

14 **MR. GORDON CAMERON:** Thank you, Mr. Forster.

15 And now Mr. Fadden, could you give us your
16 remarks?

17 **--- PRESENTATION BY/PRÉSENTATION PAR MR. RICHARD FADDEN:**

18 **MR. RICHARD FADDEN:** Good morning. Thank
19 you, and thank you for the opportunity to speak to you.

20 I should say in starting, I have a moderately
21 bad head cold, so if I sound like Donald Duck, I apologize.

22 I'm going to apologize again to the plethora
23 of lawyers, I guess including to myself as a lapsed lawyer,
24 that I'm not going to talk very much today about the law
25 governing confidentiality and openness. I acknowledge their
26 importance and the fact that if my remarks take me outside
27 that ambit, any number of people will correct me.

28 But what I'm going to try and do today is to

1 present to you a practitioner's practical perspective on this
2 topic. And I should say that over the years, I've had some
3 jobs where the emphasis was on protection and other jobs
4 where the emphasis has been on openness, so if I come across
5 as schizophrenic, it's, in fact, intentional.

6 So I think from a practitioner's perspective,
7 you start with the recognition that the law needs to be
8 respected and then you move on. In a democracy absent clear
9 constitutional or legal direction to the contrary, openness
10 and transparency is the default.

11 And I can remember that I -- we often used as
12 an example the old Soviet Union where everything was
13 classified unless there was a clear, clear indication that it
14 could be made public and that the reverse was true in Canada,
15 that everything was open unless there was clear direction
16 that it had to be kept classified.

17 I can't say that that particular perspective
18 was shared by everybody, but it sort of captured, I think,
19 the distinction between ourselves and our adversaries.

20 I think we have to acknowledge that the law
21 pushes both sides. For example, the *Security of Information*
22 *Act* pushes towards protection and the *Access to Information*
23 *Act* pushes towards openness.

24 But my first key point is that all laws and
25 policies are very susceptible to both bureaucratic and
26 institutional and personal interpretation. The Commissioner
27 wouldn't have her full-time job if that's not true. I mean,
28 we interpret at all levels within the bureaucracy, within the

1 judiciary, and this has an impact on what people do with the
2 laws and the policies.

3 And I think this is important because these
4 interpretations over time result in the creation of a culture
5 which can and does become as determinative of what's released
6 as the actual law and policies.

7 So CSIS or GAC or CSE each develop a broad
8 approach to classifying, declassifying and releasing
9 information that is unique to that institution, approaches
10 which also, as John and Al have pointed out, are also guided
11 by third party counterparts. And if you have a number of
12 institutions that have contributed to a particular piece of
13 intelligence, almost always the default is to classify to the
14 highest level sought by any given institution. It's very
15 rarely that you end up with the lowest common denominator or
16 the lowest common classification.

17 So with the possible exception of PCO, the
18 agencies we are mostly concerned about have closed personnel
19 systems, which I think reinforces this culture. And by
20 "closed personnel system", I mean you join CSIS as a boy or
21 girl spy and you want to become the Director. You join CSE
22 as a cryptologist and you want to become the Chief. And that
23 really results in a culture that's very, very, very strong.

24 Just say a couple of words about PCO, which
25 stands at some distance from other departments and agencies
26 both in terms of working for the Prime Minister, but also, in
27 the national security area, they have distance, which is
28 something that departments and agencies don't have. And it's

1 like anybody who works in a specialized area. You
2 concentrated long enough, hard enough, and you develop this
3 sort of closed world view of what you're doing, including
4 decisions to classify or declassify.

5 PCO can be very helpful. Having all the
6 clearances and whatnot, when something is important enough
7 they, ideally, are able to take a broader perspective.

8 Certainly when I was NSA, that's -- that was
9 required of us on a few occasions. You then negotiate with
10 the departments and you point out that there's often or
11 sometimes a broader perspective than that could be seen by
12 individual departments and agency.

13 So I'm not suggesting, you know, a conscious
14 desire on the part of agencies to disregard my default
15 position, but rather, a conscious effort to legitimately
16 protect information. And the balance there is, I think,
17 clearly in favour of protection.

18 I think over time the protective culture
19 becomes dominant, and this actually sits well with Ministers
20 and central agencies and senior officials, especially when
21 the protective effect, the practical effect, is reducing the
22 likelihood of controversy. I'm not suggesting that
23 controversy or partisanship very often plays a role, but if
24 by happenstance you're invoking protection under particular
25 legal provision means that you're not releasing something
26 that would call all sorts of controversy, there's nobody in
27 the system that points in the opposite direction.

28 And I'll come to this in a minute, but

1 there's no openness advocate in the entire system because the
2 Access to Information Commissioner doesn't play on these
3 highly-classified matters, so everybody sort of goes in with
4 the expectation that they're maintaining an appropriate
5 balance and, if I'm correct, the balance is sometimes tilted
6 in favour of protection because of the culture that I talked
7 about. And it often means that very, very quick decisions
8 are taken because you have the volume of material and you
9 have a culture that indicates that you're going in a
10 particular direction with respect to classification.

11 This is also true when you're getting
12 information or intelligence from the same source, the same
13 methodology or you're producing the same kinds of reports.
14 And it might be interesting for you to ask to what extent my
15 successors use algorithms as opposed to the human brain to
16 determine classifications.

17 I think that given the volume today, very,
18 very frequently -- everything's produced electronically, so
19 why not introduce an algorithm that classifies which can be
20 reviewed if appropriate or necessary by human beings, but I
21 suspect that in a lot of cases the algorithm wins.

22 And I think in the system it's important to
23 note, too, that appeals outside the system, they're
24 difficult, they're lengthy and they're expensive, so if you
25 can't get somebody within the system to respond to a request
26 for declassification, it's very difficult to get otherwise.

27 So my central point is that while much of the
28 information that you will be interested in deserves

1 protection, and John and Al have pointed out a good number of
2 reasons why, the culture, the workload and the tradition in
3 agencies, I think, is to tend towards overprotection. Not
4 always the case, but it's frequently the case.

5 Again, I want to stress the absence of an
6 openness advocate in all of this, with the possible exception
7 of the Department of Justice, which unfortunately, tends to
8 focus on the law. That's a joke, and bad one, it seems. And
9 PCO where the files, if they're important enough, they merit
10 consideration there.

11 So what I'm trying to say in my roundabout
12 way is there is room to push because of this overprotection,
13 this culture. And I don't know in the context of this
14 Commission to what extent PCO and DOJ are going to be
15 involved in individual decisions, but I would commend to you
16 the view that if you have a lot of trouble getting openness,
17 you, Commissioner, should consider talking to the Clerk of
18 the Privy Council, who is the guardian of all of these things
19 for the public service, and the statutory guardian of Cabinet
20 secrets.

21 So before suggesting a couple of ideas to
22 consider as it works its way through specific reports of the
23 Commission, let me revert to the practical and try and put
24 myself in the shoes of people who are working in the system
25 and who have to deal with all sorts of secrets.

26 And I think in the practical sense, there are
27 three kinds of secrets. There are national security secrets
28 that we've talked about this morning, there are national

1 interest secrets that have been discussed yesterday and Al
2 alluded to briefly, and then there are Cabinet secrets. And
3 everybody has to be aware of these as they work their way
4 through the classification process and the release process.

5 Each have their own rules, each have their
6 own culture, but I think for your purposes, probably the most
7 important is the national security secrets. Cabinet secrets,
8 as you know, are entirely the prerogative of PCO and nobody
9 else plays on them, or if they do it's at the risk of their
10 lives.

11 But national interest information is often
12 in the background and is often passed on to analysts in
13 access to information shops, which don't necessarily have a
14 picture of what the national security implications are. So
15 what I'm trying to say again, in my round about way, is that
16 these three categories sometimes overlap and interlock with
17 one another, and disaggregating them is an important part of
18 the process.

19 In the absence -- again, I'm repeating
20 myself, but in the absence of an openness advocate, things
21 tend to be classified more than they need to be. So a couple
22 of concrete thoughts. If you believe that what I'm saying
23 has some value, this culture bit, trying to get the
24 government to admit that this plays a role would I think help
25 you discuss on a practical level, individual
26 declassifications.

27 Agencies do get too close to their material
28 and there has to be a way to provide some distance. I don't

1 know if you have this within the Commission, but hiring
2 somebody who's recently retired and worked in this area would
3 I think, be helpful explaining the mindset of people. I know
4 people like Mr. Cameron have worked in this area for a long
5 time, but it's not exactly the same as finding a practitioner
6 who's recently retired to give you a bit of an insight.
7 Involve PCO to play the openness advocate. This should be
8 consistent with the Prime Minister's view that he wants all
9 of this information to be as open as possible.

10 I think another area that's worth thinking
11 about is our allies, our close allies, our close allies are
12 much, much more open than we are. They really protect their
13 core secrets, but the Brits, the Yanks, the Australians tend
14 to be much more open than Canada is. And you know, you can
15 often point to something that they've released that's very
16 close to what you want to release, and ask the officials, why
17 can't we do this? Al has alluded to the question of passage
18 of time. I think that's very important.

19 One of the issues that came up when I was
20 still working was -- well, let me stop for a second. I
21 suspect that you're not going to be looking that every piece
22 of raw intelligence that's produced in the period for which
23 you have a mandate, and a lot of it will be consolidated
24 analyses of one point or -- one sort or the other. And one
25 of the reasons sometimes that things are classified is
26 because the individuals, the officials, don't want to release
27 a set of information that relates to one of the things that
28 John or Al pointed out about, while at the same time, all of

1 this information is in the public domain.

2 And one of the reasons that I used to push
3 back a little bit on my colleagues is, is because within the
4 national security community, people will always prefer
5 national security collected information over the fact that
6 the economist has reported this, or it appears on CBC on the
7 evening news. I'm exaggerating slightly to make my point.
8 But if you can argue with officials that all of this
9 information is broadly speaking, public, why don't you just
10 take it from the perspective and forget about the collection
11 angle, and somewhat change your summaries or your actual
12 final analysis being presented?

13 And I think the other point I would just
14 make, and then I'll stop talking, is -- and it's a device
15 that I used in talking to parliamentary committees, is that
16 you can take a lot of intelligence and aggregate it up a
17 level. It doesn't change the substantive message, but you
18 just lose a little bit of the detail, but in the end, nothing
19 is lost.

20 And I think it's important to remember that
21 Ministers and senior officials very rarely get raw
22 intelligence. They get analytical reports. So everybody
23 getting all upset because they can't read the particular CSE
24 intercept, that you know, took place on date X from person Y,
25 that may or may not be important for the historians, but
26 Ministers, the Prime Minister and senior officials rarely ever
27 get that. They will get consolidated reports, they will get
28 analytical reports, and it's in these kinds of reports, I

1 think, where you have a little bit more flexibility to argue
2 that, you know, if you take out two words or if you aggregate
3 up a level, or if you compare them to the allies, you might
4 get them to release.

5 So I don't mean to suggest as I conclude that
6 I'm in favour of releasing everything, I think there are some
7 secrets that are -- it's absolutely critical to protect, but
8 that doesn't mean that there should not be discussions on the
9 interpretation given by officials on what particular point of
10 information can be released or not.

11 So thank you for your attention.

12 **COMMISSIONER HOUGE:** Thank you.

13 **--- QUESTIONS TO THE PANEL BY/QUESTION AUX PANÉLISTES PAR MR.**

14 **GORDON CAMERON:**

15 **MR. GORDON CAMERON:** Thank you, Mr. Fadden.

16 Gentlemen, as we all know, we will tomorrow
17 have, roughly speaking, your counterparts, plus someone from
18 PCO who are currently incumbent in positions that you held in
19 the course of your careers. And so we will have an
20 opportunity to get perhaps a more detailed account of how the
21 institution of CSIS works, how CSE works.

22 But just so that we can put the comments
23 you've made today and some of the points we might be able to
24 explore in the time left to us into context, I'd like to ask
25 each of the agencies, so to speak, to describe roughly
26 speaking, the type of work you do with a view to contrasting
27 the two of them. And in particular, people hear CSIS, they
28 hear CSE, for a lot of people I think the mere emergence into

1 the public of CSE is a relatively new phenomenon.

2 So if I could ask either or both of you, Mr.
3 Fadden and Mr. Jones, to talk about the type of work CSIS
4 does and then Mr. Forster, I'll ask you to describe the type
5 of work that CSE does, and hopefully the participants will
6 have a better perspective on what different types of
7 intelligence is originating from the two agencies.

8 **MR. RICHARD FADDEN:** Well, if I may, I'll
9 start with just a couple of general comments.

10 Al was far more involved in operations than I
11 was, but the first comment I'd like to make is the law makes
12 it very clear that CSIS must distinguish between domestic
13 intelligence and foreign intelligence. It's the sort of
14 thing that permeates the agency. In both cases you can
15 incidentally collect the other kind of intelligence.

16 But fundamentally, CSIS was created to be a
17 domestic intelligence agency. It was to worry about
18 sabotage, terrorism, sedition, and things like that. And
19 while today there's a clear shift towards being able to
20 collect foreign intelligence both here and abroad, the
21 agency, the service clearly distinguishes the two. And the
22 law requires that, and it's one of the -- I may be sol bold,
23 one of the fixations, in my view, the exaggerated fixations
24 of the Federal Court, but that's for another debate over a
25 glass of wine.

26 But that sort of view permeates everything
27 that they do, and we have to be very careful not to do that.

28 The other general statement I would make is

1 that the law allows one agency to ask another agency to do
2 something within it's mandate that it cannot technically do.
3 So CSIS regularly asks CSE to do some collection for it, as
4 long as it's clearly within CSIS' mandate. So I say this to
5 make the point that while both agencies have very clear
6 mandates, John will explain CSE's, which is more focussed on
7 foreign affairs, but CSIS can make use of CSE's technical
8 capabilities as long as it's well within it's own legal
9 mandate, and it does so on a regular basis. And in fact, it
10 can do the same of any other institution in the Government of
11 Canada.

12 So just those two macro points, along with
13 the indication that CSIS collects all of this stuff to be
14 helpful to the government. So there's always a judgement to
15 be made about what is used internally to develop broader
16 reports, and what is kicked into the system that heads up to
17 the Minister, Ministers, and to agencies around town. But a
18 lot of stuff that CSIS collects doesn't leave the agency
19 because it's too specific, it's too narrow, it doesn't really
20 apply to particular interests today. There are other things
21 -- pardon me -- there are other things that CSIS does, like
22 do security clearances and whatnot.

23 But I think I'll stop there. Al is probably
24 better equipped than I am to talk a little bit about some of
25 the more specific operational issues of what CSIS does.

26 **MR. AL JONES:** Sure. I'll start with the
27 mandate in the *CSIS Act*, which is as someone once said to me,
28 who'd come into the service from outside the public service,

1 they had never met a group of people who walked around
2 carrying their *Act* all the time like people did at CSIS. It
3 really does guide what we do on a daily basis. Because
4 everything flows from that *Act*, including all the internal
5 authorities for operational activities must reference back to
6 the *Act* itself, the section 12, which is the primary mandate
7 to collect by investigation or otherwise, the threats to the
8 security of Canada.

9 And then the specific threats under 2(a),
10 (b), (c), and (d) of the *CSIS Act*, (a) being espionage, (b)
11 being foreign interference, (c) being terrorism, and (d)
12 being subversion, which is a muted authority at the moment,
13 hasn't used in many years.

14 So the service, as Dick said, is a domestic -
15 - primarily is a domestic service, or in intelligence
16 parlance, a security service. I know the RCMP call it
17 security, but internationally, countries have what's called a
18 security service, deals with internal security. In the UK,
19 it would be MI5; United States, the intelligence part of the
20 FBI; Australia, it's ASIO, et cetera, et cetera. It has a
21 hybrid foreign intelligence mandate under section 16, where
22 the service can collect on behalf of department -- Global
23 Affairs Canada or National Defence, intelligence as foreign
24 intelligence, but only within Canada.

25 On the security intelligence side,
26 section 12, there is no geographic restriction on where CSIS
27 can operate. We protect -- service protects -- I still use
28 the royal "we" after decades of being there. The service

1 protects Canada and Canadians anywhere on the planet. So you
2 are looking at the security of Canada and Canadians at home,
3 and you're looking at the security of Canada and Canadians
4 abroad, and many of the threats against Canada emanate from
5 abroad, so you have to go where the threats are active in
6 order to get the intelligence you need to protect Canada.

7 CSIS also has, under section 21, the
8 authority to intercept private communications. This is
9 called lawful access. Tapping telephones, putting
10 microphones in walls, all these things CSIS does, publicly
11 known.

12 CSE has a tremendous technical capability for
13 signals intelligence, which is, generally speaking, outwardly
14 facing from Canada, not aimed at Canadians inside Canada.
15 But the types of intelligence that Jonathan talked to in more
16 detail than I can that CSE collect, CSIS doesn't have the
17 technical capability to do, so to support -- there is mutual
18 support, and both consume each other's intelligence. We
19 provide intelligence to CSE, which they need to help focus
20 their mandate, and likewise.

21 So that is the broader mandate of CSIS. It
22 also provides security assessments for government screening.
23 People get security clearances. CSIS does an investigation
24 based on its mandate. It also provides investigations on
25 clearances on immigration. So if people are coming to
26 Canada, they go through a CSIS check as well.

27 That's the primary overview of what CSIS
28 does. And I'll just add. There's no powers of arrest in

1 Canada or elsewhere.

2 **MR. GORDON CAMERON:** That's very helpful,
3 Jones.

4 Now, Mr. Forster, can you bring CSE into the
5 picture?

6 **MR. JOHN FORSTER:** Sure. Thanks, Gordon.

7 So the Communication Security Establishment
8 started as part of the Department of National Defence, and
9 then it received -- it became its own separate agency and its
10 own legislation. It does still report to the Minister of
11 National Defence, but is separate now from DND.

12 And it has two main focusses. One is, as has
13 been mentioned, signals intelligence, which is really
14 electronic communications in all its forms. Another
15 important distinction is its mandate is foreign, not
16 domestic. So it is not allowed to collect information
17 intentionally on Canadians, not just in Canada, but anywhere
18 in the world. And if it inadvertently comes across that, it
19 has to take steps to desensitise it and remove it.

20 It's a provider of raw intelligence, largely,
21 and it provides it to the rest of government, so CSIS, RCMP,
22 GAC, National Defence, CBSA. So it provides intelligence
23 reports for others to do their analysis and take appropriate
24 action.

25 It does have an assistance mandate. So it
26 may assist CSIS, National Defence, RCMP, to do domestic
27 operations, but they're really -- they're undertaking that
28 work on behalf of the agency and under their mandate. So

1 they're kind of a technical arm for other departments.

2 The second key part of its mandate is on
3 cybersecurity. So it protects the federal government,
4 Government of Canada's IT infrastructure from cyber attacks
5 and hackers. It recently got a mandate, not just to block
6 and prevent those attacks, but it can take steps online in
7 the global communications infrastructure to deter those
8 attacks as well.

9 And then it has the cybersecurity centre,
10 which is more the public facing arm of the -- of its mandate
11 on cyber to work with the private sector, other levels of
12 government to help them with their cybersecurity and
13 assistance and advice to Canadians.

14 And I think that kind of captures most of
15 what the CSE does.

16 **MR. GORDON CAMERON:** Thank you, Mr. Forster.

17 One point that we wanted you to just
18 describe, but it's probably something you can explain very
19 simply. But we have seen reference, and you have described
20 it yourself, that CSE collects signals intelligence.

21 First of all, can you just describe for us
22 what broadly speaking signals intelligence is?

23 **MR. JOHN FORSTER:** Yeah, sure. It's largely
24 electronic communications. So CSE, unlike CSIS, would not
25 have human sources. So it's really focussed on the global
26 communications infrastructure. It could be cell phone
27 conversations, texts, you know, computer, any kind of
28 computer communications. So it's -- it really operates in

1 that realm of the global communications infrastructure.

2 **MR. GORDON CAMERON:** And if you can explain,
3 why is it that signals intelligence tends to have special
4 designations and special treatment?

5 **MR. JOHN FORSTER:** It has certain
6 classifications because of the nature of the technology or
7 the sources of the information. So as I mentioned in my
8 remarks, some of these -- the -- you don't want to be
9 disclosing your techniques, your technology, your
10 capabilities, your sources because the targets of your
11 collection will simply take steps to avoid or block it.

12 So its techniques and its technology and its
13 access are extremely sensitive information. So reports,
14 intelligence reports you produce from those can divulge those
15 sources, as I mentioned in my opening remarks. So they take
16 steps to make sure it's very carefully -- access to that
17 information is very carefully controlled. And some of it is,
18 as I mentioned, not available to -- only a -- it's only
19 available to a handful of people in the government.

20 **MR. GORDON CAMERON:** Right.

21 Now, I'm going to move on to a different
22 topic, but Mr. Fadden or Mr. Jones, is there anything you've
23 wanted to add to the respective allocation of
24 responsibilities between the two agencies before we move on
25 to another topic? No? Okay.

26 **MR. ALAN JONES:** I'll ask you. Would you
27 want us to discuss the disclosure regime in -- for CSIS as to
28 what it does with its intelligence within the community?

1 **MR. GORDON CAMPBELL:** That's on my list, so
2 let's go there now. Yes.

3 **MR. ALAN JONES:** Yeah.

4 **MR. GORDON CAMERON:** The types of
5 intelligence reports you produce and the distribution and
6 disclosure you make within the intelligence community.

7 **MR. ALAN JONES:** Okay. So it is -- Dick and
8 I have often commented, there's not much point in spending a
9 lot of time and money collecting intelligence and then just
10 sitting there and admiring how clever you were at gathering
11 it. It actually has to become useful at some point.

12 So obviously, the service is very detailed in
13 its reporting. One of the tenets of doing good intelligence
14 work is attention to detail. So the reports are very
15 detailed. We document everything. Things -- others might
16 say, "Why would you document such -- in such details?"
17 Because you don't know in the future when that detail may
18 become relevant, and that detail may actually prove that what
19 you thought about something in the first place was wrong or
20 right. Data is somewhat self-correcting. The more of it
21 that you get the clearer the picture becomes.

22 John mentioned earlier the risk in reading a
23 singular report on a file. What you know at the outset of an
24 investigation is often quite different than what you
25 ultimately know after you explore more, do more
26 investigation, more fact finding, challenge what you know;
27 you may end up in a very different place.

28 We live in a global world where there is --

1 television is on, CNN is on all the time. My general rule in
2 running operations was the first thing you hear on the
3 television is wrong. You know? It will take time to
4 actually figure out what happened.

5 So we document everything in great detail.
6 Those reports sit in a automated database because you need to
7 be able to recover it and compare it and analyse it to other
8 data and do it quickly. And those documents, that
9 information is kept for many years because it may be years
10 before you get more clarifying information because what you
11 know suddenly comes into context.

12 I have seen many investigations where a piece
13 of intelligence collected, seven, eight, ten years ago,
14 suddenly becomes key in understanding a threat that is --
15 that has developed. That's what intelligence services do.

16 The threshold for what you collect is
17 different than a criminal investigation. For a police
18 officer, that was educated many times in the Superior Court
19 of British Columbia by judges who informed me that what I
20 believed was irrelevant, it's what I knew that was important,
21 when you were doing intelligence investigations, you gather a
22 lot of information that is at not the level of what criminal
23 evidence would be. Rumours, fractured pieces of information,
24 bits and pieces, contradictory investigation, we'll often get
25 things that are -- simply can't be two things at the same
26 time, but yet you get information saying that it is, all of
27 that sits in your database, all of it sits in reports.

28 So learning how to read intelligence is very

1 important. Learning how to understand what it is that's
2 being presented to you, as John said, is very important.

3 As Dick said, providing raw data to senior
4 decisionmakers is often not useful because you don't want to
5 turn the prime minister or a deputy minister into an analyst.
6 And I have seen circumstances in the past, which are better
7 now, where you were dealing with a crisis and the information
8 that was coming in was almost raw. And so you had deputy
9 ministers and senior officials sitting there trying to track
10 in their mind all these reports that they've seen over the
11 last two or three weeks, which, as I said, is not necessarily
12 the same every time you see it, and make sense of it. This
13 is not a helpful way to run a crisis.

14 So someone needs to do that work for our
15 seniors, and that is done. So that's why they're getting
16 assessed information, analysed information, and not just raw
17 pieces of information thrown at them.

18 We share information with other intelligence
19 services between threats are global. We need to have
20 cooperation to protect Canada. We sometimes come into a
21 section of intelligence on a threat that is developing
22 against an ally or a partner, even a country who you may not
23 have the best of diplomatic relationships with, but if you
24 find out that there is going to be, for example, a terrorist
25 attack where there is life at risk, you have an obligation to
26 try and tell other countries "this is what we know; be
27 careful." We don't want to sit on that information and allow
28 something to happen on the other side of the world, just as

1 we would hope that another country would not sit on
2 information that would identify a threat to Canadians.

3 When there is intelligence that is pointing
4 to criminal activity, and criminal activity that either rates
5 -- relates to one of those threats that I described,
6 espionage is a crime in the *Criminal Code*, terrorism is a
7 crime. We'll learn more about how much foreign interference
8 actually becomes a crime or not. That when we get
9 intelligence at that level, we have a mechanism or mechanisms
10 to advise the police of jurisdiction. In a national security
11 case, it's the RCMP. And there are mechanisms to do that.

12 We have what's called a disclosure letter.
13 There may be some changes to this. I am a little dated. I
14 am retired. We'll find out more tomorrow, I'm sure. But a
15 disclosure letter, and these terms are a bit odd for anyone
16 who is not familiar with it. There is a disclosure letter
17 and an advisory letter.

18 Disclosure letter would simply say to the
19 RCMP or police of jurisdiction, "We found out information
20 about this we think is criminal activity. You may want to
21 respond to this, but this information is ours. We're not
22 disclosing it to you for court purposes or for anything else,
23 we're just letting you know."

24 An advisory letter is a more complex process.
25 We are actually providing advice to the RCMP and saying,
26 "Here's what we know, and here's what you can use." And when
27 you say, "here's what we -- what you can use", this obligates
28 the service to do certain things, whether it's retained

1 intercepted communications, whether you document something,
2 whatever, you start to become part of that process. The
3 whole intelligence to evidence is a complicated piece. Won't
4 get into that today.

5 The service may also incidentally come across
6 information that is not related to its mandate, but may be
7 valuable to it through another part of its mandate, o -- or
8 another criminal investigation. You might discover drug
9 dealing or a bank robbery in the process of doing something
10 else, so you would want to disclose it to the police of
11 jurisdiction. "We have discovered information which relates
12 to Health Canada, which relates to the Department of
13 Environment, Department of Finance, we have a mechanism to
14 say this was incidentally collected. It's not part of our
15 mandate, we weren't looking for it. We came across this
16 information. It might be useful to you. Rather than it
17 sitting in our databases and going nowhere, we can disclose
18 this amount to you and this is what we'll agree for you to do
19 with it."

20 So that disclosure regime and those
21 interrelationships are ongoing 24 hours a day, 7 days a week.
22 They're very active. These are not occasional things that
23 you do, this is your life all day, every day in operations in
24 CSIS.

25 **MR. RICHARD FADDEN:** May I add a thought?

26 **MR. GORDON CAMERON:** Yes, please; please do.

27 **MR. RICHARD FADDEN:** I agree with everything
28 that Alan said, but just to make a further distinction. The

1 service produces report, CSE produces report, the military
2 produce reports, GAC produces diplomatic reports, and every
3 now and then, so does CBSA and a bunch of other departments.
4 There's a secretariat in the Privy Council Office called the
5 Intelligence Assessment Secretariat, which is focussed mostly
6 on things foreign, but when there's an overlap with things
7 domestic they have a mandate. So their particular mandate is
8 to consciously seek out reports and intelligence from
9 anywhere in the Canadian Government and anywhere from our
10 allies.

11 So they would take, for example, if they were
12 producing a report on foreign interference by China, they'd
13 take CSIS reports, CSE reports, they'd ask Foreign Affairs
14 whether there is anything, they'd check into what the allies
15 are saying. I think they now do open sources much better
16 than they used to. And they will put this in a consolidated
17 level report, which would most likely be the kind of report
18 that would go to the prime minister, ministers, and senior
19 officials. As Alan said, very rarely do you give very senior
20 people a specific narrow piece of intelligence.

21 More broadly, the system distinguishes, I
22 think quite consciously, strategic analytical intelligence
23 and tactical intelligence. Not that there's a rule or
24 anything, but I just want to emphasise what Alan said. You
25 don't give ministers tactical information about a terrorist
26 attack. You may tell them that one is going to happen, but
27 you don't give them the details. But you do in a strategic
28 report pull together everything you might know about the

1 origins of that potential attack, or foreign interference, or
2 whatnot, so that they can make sense of it.

3 But it might be interesting, given your
4 interest in -- I suspect your interest in what ministers and
5 prime ministers knew in the context of foreign interference,
6 to see what the IAS has produced in this context, which is
7 the prime minister's intelligence secretariat, but the
8 material is also made available to ministers and senior
9 officials. Thank you.

10 **MR. GORDON CAMERON:** And we will be hearing
11 from a representative of PCO tomorrow.

12 But that's a good segue to the next question
13 I was going to ask all of you. You've talked about the
14 process by which intelligence and information is collected
15 and made into the types of reports and intelligence products
16 that your agencies produce, and in that case, for an audience
17 that is receiving and cared to receive classified
18 information.

19 The next question for each of the agencies
20 would be about situations in which you've been called on to
21 make what will be explicitly public comments. That is,
22 you're going to be appearing in front of a parliamentary
23 committee, or perhaps you've been asked to create a briefing
24 that is going to go to cabinet or to some audience that isn't
25 an appropriate audience for the classified information, or
26 there's a report, even an annual report of your agency,
27 something like that.

28 What process do you go through, you know,

1 I'll put it to you, Mr. Fadden. You've been summoned to
2 speak to a parliamentary committee on a topic that you know
3 about almost exclusively as a result of your exposure to
4 classified information that you're about to be questioned.
5 You'd like to be able to say something more than "I'm sorry,
6 I can't answer that question." What process do you go
7 through to prepare yourself for an appearance like that?

8 **MR. RICHARD FADDEN:** I'm smiling because I
9 have been bitten by that process once or twice. I mean,
10 there are two phases to it. One is you produce written
11 comments that you make as close to what you want to say as
12 possible, and if there's anything at all controversial with
13 them, you share it with another department that might be
14 interested. But in particular, if you're a senior official,
15 if you're a deputy minister, you make sure that PCO is
16 comfortable. So that's the written document that, you know,
17 will go on the record. As is often the case, as you're going
18 to demonstrate today with your questions, often, very often
19 before a parliamentary committee, the tendency to ask for
20 more detailed information comes through questions. From
21 there, it's a matter of judgment. I've tried very hard, and
22 mostly I think I've succeeded, in doing what I suggested that
23 you do, which is I try and aggregate up classified
24 information, or sensitive information, so that you can make a
25 general statement on the topic that is -- you're being
26 queried about, and I think that's what they pay you for. If
27 you're a deputy minister, or the director of CSIS, or the
28 chief of CSE, you have to demonstrate judgment about how much

1 you can say because the general rule under all of the
2 governments for which I've worked is try to be as
3 collaborative as you can in front of parliamentary committees
4 without causing, you know, all sorts of grief with allies or
5 with the law.

6 So there's no -- you can't plan for what
7 parliamentary committees are going to ask you. So a lot of
8 it is your understanding of the broad political environment,
9 your understanding of the national security environment, and
10 the application of judgment. And I've found, I don't know if
11 John or Al's experience has been the same, that if you make
12 even the slightest effort to aggregate up and to answer
13 questions on the basis of your judgment, it works. But the
14 written material you process through the system.

15 **MR. GORDON CAMERON:** Right. And if I can
16 just ask, we've used the expression summarize or generalize.
17 Is that roughly analogous to what you're calling aggregate
18 up?

19 **MR. RICHARD FADDEN:** I guess you could. I've
20 used it mostly in the context -- in the practical context of,
21 you know, you have a report, and you just remove some of the
22 detail. I don't know if that's what you mean.

23 **MR. GORDON CAMERON:** Yes.

24 **MR. RICHARD FADDEN:** But very often,
25 classifications are determined by, you know, a word or a
26 sentence or a paragraph. And without necessarily removing
27 them, you can rewrite them to remove the detail a little bit,
28 and that goes on a lot. I mean, I -- to be honest, I spent a

1 bit of my time when I was NSA, trying to convince the
2 agencies to do that, because the higher the classification,
3 the more difficult it is to get in front of people. And as
4 both Al and I have said, the objective is to get it in front
5 of people. So by aggregation, I just mean slightly deluding
6 the detail, sometimes by shifting the wording, while still
7 being very careful that you don't lose the core message.

8 **MR. GORDON CAMERON:** Thank you. An
9 expression we've seen is "right to release"; in other words,
10 a document that is created specifically with the objective of
11 it being released to an unclassified context. Is that the
12 same thing we're talking about?

13 **MR. RICHARD FADDEN:** Not -- well, I guess in
14 the end it is, yes.

15 **MR. GORDON CAMERON:** Yes. Okay. Mr.
16 Forster, can you describe how your agency approached that
17 during your day; that is, situations where the agency had to
18 produce either a briefing to an unclassified audience, or an
19 annual report, or an appearance by you, or one of your
20 colleagues before -- in the public or before a parliamentary
21 committee?

22 **MR. JOHN FORSTER:** Sure. Well, when I
23 started at CSE, it was very -- its general practice was not
24 to disclose much of everything. In fact, it was only in the
25 '80s that the government even acknowledged it existed, so and
26 that the practice and the culture was not to say too much at
27 all. We faced some -- you know, a very healthy challenge and
28 spotlight based on unauthorized disclosures of U.S.

1 intelligence where we actually now had to go to committee and
2 talk about -- more openly about what we did, and why we did
3 it, and how we did it. And we started producing material on
4 the website that better explained. And we found that it's,
5 as Dick mentioned, a lot of the classification comes from
6 some of the details, and that don't -- aren't really
7 necessary to communicate the gist of what you're doing, or
8 what the issue is, or the event that you're trying to
9 communicate. So it's really finding a way to communicate it
10 strategically, here's the issue, here's the current state,
11 while removing a lot of the details that may disclose your
12 methodology, your technology, your sources, or embarrass the
13 country, or whatever, you know -- or not embarrass, but
14 damage your international relations.

15 So I think it -- you know, it's similar to
16 what Dick said. It's finding that right balance and there
17 were times where certainly with our staff we'd have a pretty
18 healthy exchange about what we could and couldn't say about
19 issues, and I think we advanced it, and since I was there,
20 they're even more open now, so it's been kind of an evolution
21 so.

22 **MR. GORDON CAMERON:** Okay. Now, gentlemen,
23 subject -- what I'd like to do is ask you if you have any
24 final comments because then we're going to break for about a
25 half an hour. The participants are going to see if they have
26 any questions that they'd like you to answer, and we'll
27 resume. But before we break for that Q and A process, are
28 there any comments you'd like to make to just recap or cover

1 some of the points that you've heard others talk about?

2 **MR. RICHARD FADDEN:** Just one small point,
3 and it's drawing on what I -- I'm trying to be helpful to the
4 Commission, about strategic intelligence. And I know a lot
5 of people in this country advocate for the almost total
6 release of classified information, which I don't think is
7 possible. So as I was trying to indicate earlier, the Prime
8 Minister, an official, rarely gets detailed tactical source-
9 based intelligence. He gets strategic intelligence. So for
10 those people who are asking for, you know, raw intelligence,
11 or details, I guess my thought would be why should they get
12 it when the Prime Minister doesn't, because he really doesn't
13 get it except in the most exceptional circumstances where,
14 you know, life and limb would be at risk. And I think that's
15 true of most ministers and deputy ministers most of the time.
16 Pardon me. There's this belief, I think, among some parties
17 that, you know, people go to, you know, go to the office in
18 the morning and they, you know, they read all these details
19 of, you know, what colours was the pyjamas of the Consul
20 General in Vancouver wearing and things like that. Well, it
21 doesn't happen that way. You usually get fairly highly
22 aggregated strategic intelligence.

23 So my simple point is, if it's good enough
24 for the Prime Minister, it should be good enough for
25 everybody else, except there are always exceptions. But I
26 just wanted to try and make that point. And not everybody in
27 government gets all of this detail that a lot of people
28 consider to be critical when very often it's not. Thanks.

1 **MR. GORDON CAMERON:** Thank you.
2 Commissioner, that is the completion of this session, so it
3 would be timely to take a break.

4 **COMMISSIONER HOGUE:** Yes, and we'll take a
5 longer break just to make sure that the participants have the
6 time to draft their question that they want to send to the
7 Commission counsel. Thank you.

8 So it's -- we'll be back in about 30 minutes.

9 **MR. GORDON CAMERON:** Okay.

10 **THE REGISTRAR:** Order, please. À l'ordre,
11 s'il vous plaît. The hearing is in recess for 30 minutes.
12 La séance est en pause pour 30 minutes.

13 --- Upon recessing at 11:15 a.m.

14 --- L'audience est suspendue à 11h15

15 --- Upon resuming at 11:53 a.m.

16 --- L'audience est reprise à 11h53

17 **THE REGISTRAR:** Order, please. À l'ordre,
18 s'il vous plait.

19 This sitting of the Foreign Interference
20 Commission is back in session. Cette séance de la Commission
21 sur l'ingérence étrangère a repris.

22 **COMMISSIONER HOGUE:** You can go ahead.

23 --- QUESTIONS TO THE PANEL BY/QUESTIONS AUX PANÉLISTES PAR

24 MR. GORDON CAMERON(cont'd/suite)

25 **MR. GORDON CAMERON:** Gentlemen, we have a
26 number of questions, a good number of questions, probably
27 more than we have time to address them all individually, but
28 helpfully, in a way, many of the same questions were asked by

1 different parties so we're doing our best to amalgamate them
2 together or aggregate them, as you would say, Mr. Fadden,
3 into single questions.

4 Let me begin with one which we've received,
5 as I say, in various forms from several parties, but I'll use
6 one of the formulations to put the question to you.

7 It's probably a question that's more likely
8 to have arisen in the context of CSIS and CSE, but Mr.
9 Forster, we'd welcome your views on this as well, which is
10 how do your agencies approach considerations around
11 intelligence you've received that might suggest that an
12 individual is under threat or potentially is a target of
13 foreign interference, and specifically, if that individual is
14 a parliamentarian?

15 What would you do when you got that
16 intelligence and how would you approach possible disclosure
17 issues in relation to that?

18 **MR. RICHARD FADDEN:** Well, let me take a stab
19 at it, if I may.

20 One, I would make the point that what would
21 happen today is not what would have happened in my day. I
22 think the current government has broadened considerably the
23 instructions they've given to CSIS in particular about
24 forewarning people who may be threatened.

25 But in my day, when I was in CSIS, if I had
26 found out that somebody was under threat, parliamentarian or
27 not, I would have found a way to do something about it. And
28 I don't say that lightly.

1 If it were a parliamentarian, I would have
2 made sure my Minister knows about it and that the Privy
3 Council knew about it. If it was another person, you know,
4 my colleagues and I would have consulted and decided if it
5 was a physical threat, you have to bring in the police
6 because, at the time, the service didn't have the ability to
7 affect physical activities, but rightly or wrongly, I've
8 always thought that CSIS had a mandate to deal with threats.

9 Most of them were systemic or national-level
10 threats, but if individuals were threatened, we would have
11 found a way to do something about it. The more political it
12 was, the more we would have made sure that Ministers know
13 about it.

14 Is that a fair thing to say, Al?

15 **MR. ALAN JONES:** Absolutely.

16 If it involved a physical criminal threat, or
17 threat, threatening is a criminal activity, that would be
18 involved police jurisdiction, usually the RCMP and any
19 contact would go through the RCMP. But the disclosure to a
20 parliamentarian is governed at the headquarters level, it's
21 not something just regional. It would be done locally, a
22 local decision in consultation and probably up through PCO to
23 start with, which also deals with the security of
24 parliamentarians and cabinet ministers.

25 **MR. GORDON CAMERON:** Now, Mr. Forster, if
26 your agency received intelligence to that effect, how would
27 it be handled?

28 **MR. JOHN FORSTER:** Right. So again, remember

1 ours was the ---

2 **MR. GORDON CAMERON:** Oh, got an audio
3 problem.

4 **MR. JOHN FORSTER:** Hello, can you hear me?

5 **MR. GORDON CAMERON:** There you go. We got
6 you now.

7 **MR. JOHN FORSTER:** Sorry. Remember ours is a
8 foreign mandate. So we'd pick that up through foreign
9 collection. The CSE has a series of what they call crows.
10 They're sort of people who just take very sensitive
11 intelligence around to different departments to make sure
12 they've got access and have read it. So we definitely would
13 flag that with a couple of the crows to make sure that that
14 intelligence was read and understood by some of the key
15 agencies.

16 And depending on the target -- since it's a
17 threat and a target, I would want to make sure my colleague,
18 the Director at CSIS, and the National Security Advisor were
19 personally aware of it. Because again, CSE isn't -- doesn't
20 take action on the intelligence, they're a collector of it.
21 But I would certainly want to make sure that the proper
22 agencies who would respond to it were personally aware of it
23 at the very senior level.

24 **MR. GORDON CAMERON:** Okay. Thank you.

25 Gentlemen, during your discussion, and this
26 was particularly a point that Mr. Jones and Mr. Fadden made,
27 you talked about intelligence over time becoming -- the
28 disclosure of the intelligence becoming less injurious over

1 time as it gets older. And the question is, could you expand
2 on that? Is that invariably the case, or is there some
3 intelligence that the confidentiality of which survives the
4 passage of time?

5 **MR. ALAN JONES:** It would be the latter. The
6 -- it's no invariably, it's case by case. As I said, there
7 are some circumstances which protection of the source,
8 particularly human source, would endure for the lifetime of
9 that source. There are other times when the circumstances
10 have changed around that human source, or other circumstances
11 which would mitigate those threats.

12 With a technical source, it's very similar,
13 but not necessarily the same. I'll talk to a section 21
14 warrant that the service would have intercepting the phone or
15 whatever. That would be top secret, the fact that that
16 intercept would exist. It is highly protected, don't reveal
17 that it's happened.

18 After a period of time, if you no longer have
19 that intercept and there's no technological barrier, the risk
20 to revealing that information would be mitigated, unless of
21 course, you had a human source involved in the deployment of
22 that -- of that technology. But it's more likely to happen,
23 but not as an absolute rule, more likely to happen with a
24 technical source than a human source.

25 And I would add to that where the CSIS sits
26 in a different world than police, police notify people after
27 they've intercepted their phone, after a period of time,
28 unless there's reason to continue protecting it under part 6

1 of the *Criminal Code*. That's very a different regime.
2 Right?

3 **MR. GORDON CAMERON:** Very different in the
4 sense that the person is never told when there's been a CSIS
5 interception?

6 **MR. ALAN JONES:** Another question about some
7 of the answers you gave in our session earlier this morning,
8 and Mr. Fadden, in particular, you noted that the PM doesn't
9 get raw intelligence but rather strategic assessments without
10 all of the technical details. And the question is, is the
11 suggestion here that the Prime Minister is missing important
12 parts of the picture when he or she makes their decision?

13 **MR. RICHARD FADDEN:** No, I don't think so.
14 And if I didn't, I should have said there are always
15 exceptions to that rule. I can think of one instance that I
16 can remember where I gave a Prime Minister something from
17 John's old shop, because it was particularly relevant to
18 something that was quite sensitive. But very, very rarely.

19 And as I think all of us were trying to say,
20 a lot of intelligence, including intelligence that has a
21 physical outcome, is built up over time. It's rarely one
22 single piece. It's rarely one source, you know, that tells
23 the whole story. So the objective in dealing with Ministers
24 and the Prime Minister is to pull all of these together so
25 that they can understand what happened. There may be a list
26 behind, you know, an annex which sort of says, you know, this
27 has been going on since time X to time Y, and give some sense
28 of where we got the information.

1 But no, I absolutely don't think that's the
2 case. And to support that view, in all the times that I've
3 worked with Ministers and Prime Ministers I can only think of
4 one instance where I was asked to provide the raw
5 intelligence. So I think if it had been a real issue with
6 Ministers, we would have been asked much, much more
7 frequently.

8 **MR. GORDON CAMERON:** All right.

9 **MR. ALAN JONES:** Could add just one thing to
10 that? Is when you are disclosing the -- or briefing up on
11 any of these issues, at the front of your mind is, why are
12 you telling this person what you're telling them? Because
13 most -- whether it's a Prime Minister or any senior leader in
14 your organization, usually the first thing they'll say is,
15 why are you telling me this and what is it you expect me to
16 do about it? So these are policy decisions, you're briefing
17 up because it's impacting policy, you're not looking for
18 operational direction or operational input.

19 So that would put into context the type of
20 aggregated information or analyzed information, is why are
21 you briefing the Prime Minister on this?

22 **MR. GORDON CAMERON:** Again, on this point. I
23 think it arose out of some of the comments you made this
24 morning, Mr. Fadden, about a higher-level aggregated
25 information being more -- more appropriate for disclosure.
26 And the question was, are you proposing that the Commission
27 ask the government to prepare such reports for the purposes
28 of its use in this inquiry? Or is it that they should be

1 looking for the higher-level aggregated reports?

2 **MR. RICHARD FADDEN:** No, I certainly wasn't
3 suggesting that new reports be prepared. A, it would, you
4 know, with the passage of time it might give a different
5 impression. But I think you'd probably gridlock the system
6 if you started asking for these on a systematic basis.

7 What I was suggesting is that if you have a
8 particular report that you wanted made public and the
9 government is not readily accepting your request, making a
10 suggestion or asking them to make a suggestion on an existing
11 report about how to aggregate up a level or two might be a
12 way to go. But certainly not to create a new report.

13 **MR. GORDON CAMERON:** And again, a number of
14 questions about -- presumably arising in part out of some of
15 the information that we've received -- that the Commission
16 has received over the last few days about the role of the
17 public interest in disclosure, and weighing the importance of
18 confidentiality for national security purposes, and the
19 public interest in disclosure.

20 Where would that fit into the analysis in
21 your agency's consideration of potential disclosures? Where
22 if ever within your agency, would you be assessing the
23 importance to the public of knowing this information when
24 you're deciding what to disclose to the public?

25 **MR. RICHARD FADDEN:** Well, in theory it takes
26 place at every level. But in practical terms, I'm not sure
27 it can be, you know, utilized equally every time a piece of
28 information is classified.

1 My sense is that, you know, this issue
2 becomes important when for some reason or other it -- the
3 file is raised. It may be for legal reasons, it may be for
4 tactical reasons, it may be for policy reasons, it may be
5 because there's a media interest.

6 But as a general routine, you know, the
7 individuals who classify reports are quite junior and they
8 have a series of criteria, and they apply them, or the
9 computer applies them for them. And answering the question
10 that you pose can either take place because an individual
11 file is pulled, and you know, a more senior person is asked
12 to focus on it. Or because there's a declassification
13 process that's ongoing, and that takes place in headquarters
14 at a fairly senior level.

15 In other words, the authority to classify
16 information is fairly widely delegated. The authority to
17 lower the classification, or to declassify it is much, much
18 less widely delegated and it would be restricted to
19 headquarters. And if a matter were at all sensitive, it
20 would go to quite senior levels.

21 **MR. ALAN JONES:** If I could add, from an
22 operational perspective, when there is a judicial, quasi-
23 judicial process and a request for disclosure, there are
24 specialized areas, policy and legal, that deal with those,
25 that process. It is not dealt with by the operational area.
26 So even as a senior operational leader, I would never have
27 been asked how much do you want redacted and how much do you
28 want left in the clear. That would not be an appropriate

1 question for me to become involved in as an operational
2 manager. That would be managed by those who were managing
3 the relationship with the judicial proceeding or whatever.
4 You might be asked what to do a damage -- a potential damage
5 assessment around specific pieces of information if they were
6 to be disclosed, what is the risk associated to that, but you
7 would not be asked in the operational sense should or
8 shouldn't we be disclosing to the maximum or the minimum.
9 That is handled otherwise, and those decisions are made
10 there. I'm not sure if that's useful, but that's ---

11 **MR. GORDON CAMERON:** Yes, thank you. Mr.
12 Forster, did you -- this seems -- the area of balancing the
13 public interest seems to arise more at the -- more downstream
14 from the agency you were in, but do you have anything to add
15 to that?

16 **MR. JOHN FORSTER:** Yeah, I would agree with
17 both Dick and Alan's comments. The other two layers in this
18 I think that are important, depending on the sensitivity and
19 the views of the inquiry and the originator, the Department
20 of Justice would also play a role in this if they felt that
21 the agency was maybe not disclosing everything it could. The
22 justice lawyers would also intervene and make sure -- provide
23 a bit of a challenge to it, have you considered this. And as
24 Dick said, I think as it -- it would get elevated to a
25 reasonably senior level to make sure that there's a broader
26 perspective taken to it than just the subject matter expert
27 who would have more of a narrow kind of focussed view on, you
28 know, does this disclose my source, or my information, or my

1 technique. So the Justice and PCO would also, you know, play
2 a bit of a challenge function there, or should play a bit of
3 a challenge function there to the agencies to make sure that
4 the broader public interest and views are also considered.

5 **MR. GORDON CAMERON:** Thank you. And we had
6 several questions arising out of your comments, Mr. Jones,
7 with respect to what went on in the Arar Inquiry, and in
8 particular, whether we have lessons to learn from that
9 process, and as I'll phrase one of the questions, do you
10 think the matter was adequately described by Professor West
11 yesterday or do you have anything to add to that?

12 **MR. ALAN JONES:** I don't have anything to
13 add. I think Professor West did an excellent job of
14 outlining the relevant part of Arar for -- regarding
15 disclosure and the process.

16 **MR. GORDON CAMERON:** Now some questions about
17 -- for either Mr. Jones or Mr. Fadden about the division
18 within your agency between -- this came out of your
19 discussion of the terrorism investigations, but we are here
20 in a foreign interference context, so could you describe how
21 your agency divides its functions as between investigations
22 of those two fields of interest, between terrorism and
23 counterintelligence or foreign interference?

24 **MR. ALAN JONES:** I mentioned earlier that the
25 *CSIS Act* defines a lot of how CSIS operates and how it's
26 organized. Section 2, finding threats, A, B, C, and D. You
27 essentially have operational branches and operational branch
28 that deals with A, which is espionage, C, which is terrorism,

1 which is the big, you know, a big file. The foreign
2 interference file tends to fall more under the A section,
3 although it's at section B of the Act as a specific threat.
4 It has never been a particularly large program within the
5 service. Counterterrorism, obviously, dominated for decades
6 the investigative capabilities and resources of the service.
7 CSIS always maintained operational capability under 2-A and
8 2-B, primarily in its counterintelligence branch. Even
9 during the years post-9/11 when counterterrorism became
10 everything for many agencies, the service maintained a
11 capability, albeit reduced, on its espionage and its foreign
12 intelligence -- foreign interference investigations while
13 some of our allies reduced theirs to almost nothing, to a
14 nub. And, in fact, over a period of years, as other larger
15 agencies in other countries began to get back into the
16 espionage and foreign interference areas, they did approach
17 the service because they were aware that we had maintained
18 some capability, reduced from what it had been, but we did
19 not turn the lights out, so to speak, on that program. And
20 that meant we could keep expertise, language capabilities,
21 knowledge and some continuity on those files even while the
22 service was under tremendous pressure with counterterrorism
23 program. But they are kept separate.

24 There are, of course, some areas where
25 foreign interference overlaps with the terrorism program.
26 There are some countries which are involved in state-
27 sponsored terrorism who play in the peripheries of other
28 terrorist activities. So you have a terrorist investigation,

1 but yet they do engage in political meddling in Canada at the
2 same time. So that's a time that was a shared responsibility
3 between some of the counterintelligence branch and the
4 counterterrorism branch, and sometimes you just make
5 arbitrary decisions as to which branch will hold that file,
6 but there is sometimes an overlap.

7 **MR. RICHARD FADDEN:** Can I add a thought?
8 Just about foreign interference. Essentially, rather
9 difficult to deal with because it means a desire to influence
10 under the radar. So if you look at the spectrum of human
11 contact between just a social gathering and foreign
12 interference with a threat of violence, you have a whole
13 bunch of things in the middle including diplomacy. So in the
14 case of terrorism, you know, if anybody's putzing around with
15 a bomb or something like that, it's pretty clear you need to
16 pursue it. But if the Consul General of country X is talking
17 to somebody over lunch, it could be foreign interference of
18 the worst sort, or it could be a social meeting where they're
19 sort of saying, well, you know, our two countries should get
20 together and agree on this particular policy. So if there's
21 no threat of violence involving the diaspora at issue, simply
22 catching people, you know, who are engaged in active foreign
23 interference of one sort or the other is in some ways more
24 difficult than terrorism where you have sort of something
25 kinetic to deal with because in many ways you're just dealing
26 with conversations. There could be implied threats. There
27 could be implied benefits and whatnot. But in many cases, I
28 think service or the RCMP have discovered FI efforts simply

1 because they related, as Al had said, to other inquiries.

2 So I just want to stress that, you know,
3 people who say, well, you know, it's obvious, you know, that,
4 you know, the Consul General of country X was talking to
5 somebody, it's foreign interference, well, it isn't obvious.
6 It's part of the job of diplomats. I was a diplomat briefly
7 early in my career and it was my job to go out and try and
8 influence that country. So finding where it's situated on
9 the spectrum is actually quite difficult to do. And not
10 unreasonably, Canada doesn't want to offend foreign
11 governments unnecessarily. So you have to find something to
12 hook on before the service or the RCMP can become actively
13 involved.

14 So all I'm trying to do is to suggest that
15 there's a spectrum here, and before you can become actively
16 involved, you have to make sure that there's a serious
17 possibility of foreign interference. And as Alan suggested,
18 sometimes it's easier if you're -- it's connected with
19 another investigation.

20 **MR. ALAN JONES:** And if I add to that, it
21 gets even more complicated when countries use proxies and
22 non-diplomatic actors to carry out foreign interference
23 campaigns.

24 **MR. GORDON CAMERON:** Can you elaborate on
25 that, Mr. Jones?

26 **MR. ALAN JONES:** Well, foreign journalists
27 sometimes, certain media representatives could be part of a
28 state campaign. I mean, to be very specific, I have a

1 certain amount of exposure to the activities of the Republic
2 of China in foreign interference in Canada. They had a
3 multi-prong -- they have a multi-prong approach. It might be
4 diplomats at the Consulate, but it might be trade
5 representatives, journalists, tourism groups who are just
6 individuals coming to Canada. It may happen in -- the
7 interference may actually happen in China itself, where they
8 have coercive abilities because they can reach families or
9 reach -- meet dual citizens who are travelling to China and
10 back to see family or to do business. So it's not just
11 simply, as Dick said, what defines an aggressive political
12 campaign, or aggressively standing up for your country, or
13 aggressively trying to get economic -- do economic lobbying.
14 At which point does it become foreign interference and
15 meddling? Clearly, if it's interfering with an election,
16 well, that's -- you know, that's -- you're into that category
17 where, like, terrorism, it's pretty clear if someone puts a
18 bomb somewhere. But the gradience between that something
19 that stark and benign or acceptable activity, it's --
20 activities, there's a lot of activities in the middle.

21 **MR. JOHN FORSTER:** Can I just add a point as
22 well on this?

23 **MR. GORDON CAMERON:** Please do.

24 **MR. JOHN FORSTER:** Yeah. Just the other
25 element of foreign interference is, not so much the human
26 context inside Canada, or whatever, but the online campaigns
27 that are waged. So disinformation campaigns that could be
28 state sponsored. The very attribute -- so CSE would be

1 trying to track and report on that activity. It's very
2 difficult. You can, you know, send that stuff through
3 umpteen number of servers around the world to cover its
4 source, or they'll -- countries may use third parties to do
5 it on their behalf. But there's a disinformation component
6 to the foreign interference, foreign influence that shouldn't
7 be forgotten, and that will only get more difficult as AI
8 technology advances further.

9 **MR. GORDON CAMERON:** Thank you. Now -- thank
10 you, Mr. Forster, for bringing us, I think -- I want to bring
11 the discussion we've just had back to the question of what
12 can be disclosed. How do we deal with the information that
13 the Commission's going to be looking at, and get as much of
14 it out to the public? And the question that we were touching
15 on earlier is balancing the public interest, et cetera.

16 And a question that's come in from several
17 different parties in different ways is, whether it would be,
18 and if so, how it would be important for the Commission to be
19 in touch with diaspora communities to get their perspectives
20 on foreign interference and how it affects them, and thus,
21 how it might affect the public interest in disclosure of the
22 intelligence about foreign interference?

23 **MR. RICHARD FADDEN:** Well, to be blunt, I
24 think if you don't develop an interest in diaspora points of
25 view, I think you will be missing an important component of
26 your mandate. I mean, the threats to, you know, diaspora
27 communities for the purpose of advancing, you know, foreign
28 state objectives I think is becoming increasingly clear.

1 And one of the difficulties that we have is
2 that most members of these diasporas come from a background
3 where dealing with the police or the security services is the
4 last thing they want to do. So even though they are
5 threatened, they feel badly, they want to do something, you
6 know, calling up CSIS or the RCMP, or anybody else, given
7 their experience with security services back home, is not
8 something they want to do.

9 So we don't have as many of those contacts as
10 I think we should have. So I would very much urge the point
11 of view that the Commission should have an active outreach
12 program, and possibly one that provides them with
13 confidentiality because people are scared. I'm generalising.
14 Not everybody is, but you know, members of some diasporas are
15 just plain scared.

16 I would argue also that one of the things
17 that government should do, and I hope the Commissioner will
18 consider this in her recommendations, is to develop a means
19 for diaspora community members to communicate with the
20 government confidentially because walking into an RCMP
21 substation or to a CSIS regional office, they don't want to
22 do by and large. And so the only time we find out about this
23 is when something goes very wrong so it's too late to do
24 anything about it.

25 So long answer to your short question, but I
26 very much hope that you don't miss the opportunity of
27 speaking with diaspora representatives.

28 **MR. GORDON CAMERON:** Mr. Jones, do you

1 have....

2 **MR. ALAN JONES:** I agree with that. I have
3 nothing to add.

4 **MR. GORDON CAMPBELL:** Yes.

5 And Mr. Forster?

6 **MR. JOHN FORSTER:** Yeah, I would certainly
7 echo Dick's comments.

8 **MR. GORDON CAMPBELL:** Okay.

9 Commissioner, I am in the happy situation of
10 having completed all of the questions that the parties
11 submitted, though in many cases they were aggregated
12 together. Some of them will be punted to tomorrow's panel,
13 where we have the incumbent equivalent of these gentlemen,
14 and the questions will be more appropriate for them.

15 But with that said, that is as much as I have
16 for this panel.

17 **COMMISSIONER HOGUE:** So thank you. I imagine
18 everyone will be happy to be free for lunch and for the
19 afternoon.

20 So see you all tomorrow morning at ten.

21 **THE REGISTRAR:** Order, please. À l'ordre
22 s'il vous plaît.

23 This sitting of the Foreign Interference
24 Commission has adjourned until ten tomorrow. Cette séance de
25 la Commission sur l'interférence étrangère est levée jusqu'à
26 10 h demain.

27 --- Upon adjourning at 12:20 p.m.

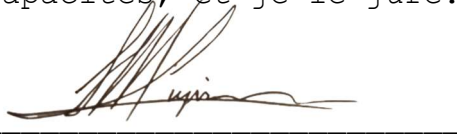
28 --- L'audience est ajournée à 12h20

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

C E R T I F I C A T I O N

I, Sandrine Marineau-Lupien, a certified court reporter,
hereby certify the foregoing pages to be an accurate
transcription of my notes/records to the best of my skill and
ability, and I so swear.

Je, Sandrine Marineau-Lupien, une sténographe officiel,
certifie que les pages ci-hauts sont une transcription
conforme de mes notes/enregistrements au meilleur de mes
capacités, et je le jure.



Sandrine Marineau-Lupien