

CANADA / JUDGMENT

R. v. Ali, Boparai & Malonga-Massamba

2020 BCSC 1309

COURT

Supreme Court of British Columbia

DECIDED

3 September 2020

Source: bccourts.ca · Research copy typeset by Esheria. Not court-issued or certified.

2020 BCSC 1309 R. v. Ali, Boparai & Malonga-Massamba

IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation:

R. v. Ali, Boparai & Malonga-Massamba,

2020 BCSC 1309

Date: 20200903

Docket: 28709

Registry: Vancouver

Regina

v.

Mustapha Mohammed Ali, Pashminder Boparai,

Moeen Khan, and Noebin Jeffrey Malonga-Massamba

Restriction on publication: Pursuant to subsection 648(1) of the Criminal Code, no information regarding this portion of the trial shall be published in any document or broadcast or transmitted in any way before the jury retires to consider its verdict.

Before: The Honourable Mr. Justice Ehrcke

Oral Reasons for Judgment

Re: Voir Dire - Application #4 "CATSA Application"

Counsel for Crown:

Rusty J. Antonuk

Michael Barrenger

Counsel for Mr. Ali:

Counsel for Mr. Boparai:

Counsel for Mr. Malonga-Massamba:

Brent V. Bagnall

Troy D. Anderson

Gloria M. Ng

Trudy Au

Brent Anderson

Place and Date of Trial:

Vancouver, B.C.

July 2-3, 20, 23-24, 2020

Place and Date of Judgment:

Vancouver, B.C.

September 3, 2020

Table of Contents

I. introduction. 2

II. evidence on the voir dire. 4

Sergeant Renard. 4

Eric Lalonde. 8

Francie Lagadyn. 9

Kelsey MacTavish. 10

III. legislative framework. 11

The Privacy Act 11

Personal Information Protection and Electronic Documents Act 12

IV. policy framework. 14

YVR Airport Authority Privacy Policy. 14

CATSA Privacy Policy. 15

V. charter section 8 and the right to privacy. 15

VI. application of CHARTER SECTION 8 in previous cases. 18

VII. the totality of circumstances test in the present case. 21

Subject Matter of the Search. 21

Direct Interest 23

Subjective Expectation of Privacy. 23

Objectively Reasonable Expectation of Privacy. 26

(a) The Place where the Search Occurred. 26

(b) Was the Informational Content in Public View?. 28

(c) Had the Informational Content Been Abandoned?. 28

(d) Was the Information in the Hands of Third Parties and Was it Subject to an Obligation of Confidentiality?. 29

(e) Was the Police Technique Intrusive in Relation to the Privacy Interest?. 30

(f) Was the Use of This Evidence Gathering Technique Objectively Unreasonable?. 30

(g) Did the Informational Content Expose Details of the Claimant's Lifestyle, or Information of a Biographical Nature?. 31

VIII. conclusion. 33

I. introduction

- [1] This is an application by the accused Mustapha Mohammed Ali and Noebin Jeffrey Malonga-Massamba (the "Applicants") for a declaration that certain still images, CCTV video, and boarding pass data regarding their June 12, 2018 flight from Ottawa to Vancouver was obtained by the police in breach of their rights under s. 8 of the Canadian Charter of Rights and Freedoms. Pursuant to s. 24(2) of the Charter, they seek an order for exclusion of this evidence from trial. The parties have referred to this application as "Application #4" or the "CATSA Application."
- [2] Mr. Ali and Mr. Malonga-Massamba are jointly charged with Pashminder Boparai on Indictment 287901 with conspiracy to commit murder between June 4 and June 19, 2018. Mr. Ali and Mr. Malonga-Massamba are also charged with firearms offences on the same indictment.
- [3] The charges arise out of a Vancouver Police Department ("VPD") investigation of drug trafficking and gang conflict called "Project Territory". As a part of that investigation, police obtained a judicial authorization to intercept private communications. In those intercepts, Mr. Boparai was overheard communicating about a "black guy" coming from Ottawa. He also spoke about needing a driver and a shooter that could be flown out from Ottawa. There was

a discussion of preparing an apartment for them, and an address at 2289 Yukon Street was mentioned.

- [4] Police obtained still photographs from CCTV footage of the elevator and lobby of the apartment building at 2289 Yukon Street, which depicted dark-skinned males in the company of two of the targets of the on-going police investigation.
- [5] Sgt. Renard was tasked with identifying those males, as it was believed they had come to Vancouver to commit violent offences in conjunction with some of the wiretap targets.
- [6] From the Canadian Air Transport Security Authority ("CATSA"), Sgt. Renard obtained still images of Mr. Ali, Mr. Malonga-Massamba and another man at the Ottawa airport ("YOW"). He also obtained boarding pass information for the three men. From Securiguard Services LTD. ("Securiguard"), Sgt. Renard obtained video images of their arrival at Vancouver International Airport ("YVR").
- [7] Mr. Ali and Mr. Malonga-Massamba now apply for a declaration that because Sgt. Renard obtained this material without prior judicial authorization, their rights under s. 8 of the Charter to be secure from unreasonable search and seizure were infringed.
- [8] The jury trial in this matter is not scheduled to begin until next year, and it is unlikely that I will be the trial judge. However, I have been assigned by the Associate Chief Justice to hear this and other pre-trial applications as the Case Management Judge pursuant to s. 551.1 of the Criminal Code.
- [9] This application was heard in a Voir Dire at which both viva voce and affidavit evidence was led. This included the affidavit and cross-examination evidence of Sgt. Renard, Francie Lagadyn, Kelsey MacTavish, Eric Lalond, and Alyssa Fazio, as well as various documents. That evidence may be summarized as follows.

II. evidence on the voir dire

Sergeant Renard

- [10] Fraser Renard is a Sergeant with the Port Moody Police. In 2018 he was involved in the VPD Project Territory investigation into criminal organization drug trafficking. A wiretap authorization was obtained on February 13, 2018.
- [11] In his affidavit, Sgt. Renard described the state of the Project Territory investigation as of June 14, 2018, as follows:
 - Mr. Ali and Mr. Malonga-Massamba were not known to police at the time, nor were they named anywhere in the wiretap affidavit.
 - On May 11, 2018, intercepted communications revealed that one of the named wiretap targets, J.V., communicated with his associate Mr. Boparai. They talked about a "black guy" coming from Ottawa. Mr. Boparai said that he would find a place for "them" to stay and take care of "them".

- The murder of two young men in Surrey on June 4, 2018 raised concerns that some of the wiretap targets may engage in violent activities.
 - On June 8, 2018, Mr. Boparai was intercepted speaking to two named wiretap targets, K.G. and G.K. Mr. Boparai spoke about going around with a "bunch of niggers" and locating people. They appeared to talk about burning vehicles. Mr. Boparai spoke of needing a driver and a shooter - a two-man team, as he put it. Mr. Boparai said that the "niggers" were from out of town; they did not know Mr. Boparai's name, or anybody else's name, or where they lived.
 - Shortly thereafter, the same three men talked about getting the black males a rental. They referred to them flying from Ottawa. G.K. would get the place ready. The black males would be given walkie-talkies.
 - Intercepts from June 11, 2018 indicated that K.G. was preparing an apartment at 1707 - 2289 Yukon Street. The context strongly suggested that the apartment was being prepared for the black males coming from Ottawa.
 - Pursuant to a judicial order, the VPD had obtained Mr. Boparai's call records, which identified numerous contacts with a number having an Ottawa area code. The contact occurred around June 12, 2018. Subscriber information from Rogers indicated that the subscriber was a "Jason Williams."
 - On June 14, 2018, the VPD reviewed June 12, 2018 CCTV video from 2289 Yukon Street, that showed K.G. and G.K. with three black males in the elevator going to the 17th floor of that building.
- [12] Sgt. Renard deposed that on the basis of this information, he believed the three black males had come to Vancouver for the purpose of committing violent offences in conjunction with some of the wiretap targets.
- [13] On June 14, 2018, Sgt. Renard was assigned the task of identifying the three black males. He deposed that he believed the men had travelled from YOW on a flight arriving at YVR around 8:00 p.m. on June 12, 2018.
- [14] Sgt. Renard said he did not know who the men were and he believed he had exhausted all other means of ascertaining their identity, although in cross-examination counsel suggested there were other avenues he could have explored, such as a "Fan Out" or cross-reference of associates through the PRIME database. Sgt. Renard testified that those other avenues were not timely enough.
- [15] On June 14, 2018 at 10:51 a.m. Sgt. Renard emailed a disclosure request form to Darlene Parker at CATSA, requesting information pertaining to "Passengers from an inbound flight into YVR from Ottawa on June 12, 2018 at approximately 20:00 hours" and indicating that he would forward pictures of the individuals. He indicated that the request was being made under exigent circumstances as he believed that the three black males were in Vancouver for the purpose of committing violent offences. On cross-examination it was suggested that

he did not truly believe in the urgency of the situation, but I do not doubt Sgt. Renard's testimony in this regard. In any event, the Crown is not relying on exigent circumstances to justify the search and seizure in this case.

- [16] Shortly after sending the email, Ms. Parker phoned Sgt. Renard asking him to resubmit the disclosure request form to include in the "Justification" field the Criminal Code section that was being investigated, and to indicate that all other avenues to identify the three males had been exhausted. Sgt. Renard understood from talking to Ms. Parker that CATSA could not provide information about security incidents and that the information would only be from the Boarding Pass Scanning System ("BPSS") and Closed Circuit Television ("CCTV") footage.
- [17] At 11:40 a.m. Sgt. Renard sent an email with a revised disclosure request form, in which he stated that the request was "Pursuant to Lawful investigation in accordance to Section 465(1) (a) of the Criminal Code of Canada". Under "Justification" he wrote: "It is believed they have used air travel. All avenues have been exhausted and receiving information pertaining to passengers' information has become time-sensitive and considered an exigent circumstance."
- [18] At 11:53 a.m. Sgt. Renard sent a third email attaching two photographs of the three black males, which he understood were from the June 12, 2018 CCTV video of 2289 Yukon Street.
- [19] A few minutes later, Sgt. Renard contacted the Security Operations Centre ("SOC") at YVR and spoke to Francie Lagadyn, telling her that he needed help acquiring CCTV footage for three male passengers on an inbound flight from YOW on June 12, 2018 at approximately 20:00 hours. He told Ms. Lagadyn that based on the time, he believed it was either a WestJet or Air Canada flight, and at 12:08 p.m, he sent Ms. Lagadyn copies of the same two pictures that he had sent to CATSA. Ms. Lagadyn provided information that WestJet Flight 609 arrived on June 12, 2018 at 19:51 hours at Gate B14, and Air Canada Flight 345 arrived on June 12, 2018 at 20:16 hours at Gate 47.
- [20] Ms. Lagadyn reviewed the CCTV footage from both flights and determined by reference to the two pictures that the three male passengers had arrived on Air Canada.
- [21] At around 1:00 p.m., Sgt. Renard met with Ms. Lagadyn at YVR. After filling out a form provided by SOC of YVR, he reviewed the CCTV footage and he noted the following:
- At 20:16 hours: Air Canada plane arrives;
 - 20:26 hours: The three male passengers are observed on the 'jet bridge';
 - 20:34 hours: The three males at the carousel picking up baggage; and
 - 20:39 hours: The three males exit the airport and are picked up in a vehicle,
- believed to be a Toyota Highlander - BC licence plate unknown.

- [22] The CCTV footage showing the three males was from areas of the airport open to the general travelling public.
- [23] In reviewing the CCTV footage, Sgt. Renard formed the belief that the three male passengers were the same three males observed in the elevator at Yukon Street with G.K. and K.G.
- [24] At approximately 2:30 p.m, Sgt. Renard obtained a copy of the CCTV footage as well as still photographs related to the movement of the three men at YVR.
- [25] When he returned to his office, Sgt. Renard had an email from Eric Lalonde of CATSA with the BPSS results identifying the three male passengers. The information in the email included the names of the three men, and that they were all on Air Canada Flight AC 0345 with a scheduled departure from YOW Gate 13 at 18:00 hours on June 12, 2018. It also listed the time and place that each boarding pass was scanned.
- [26] In cross-examination, Sgt. Renard identified a copy of a General Warrant that Det. Cst. White had obtained on July 11, 2018 for boarding pass information and photographs of six individuals in relation to flights through YVR.

Eric Lalonde

- [27] Eric Lalonde, a SOC Team Leader of CATSA, deposed that CATSA is a Crown corporation whose mission is protection of the public by securing critical elements of the air transportation system, including screening passengers and their belongings. His role as Team Leader included receiving approved disclosure requests and searching for the requested information in the BPSS and CCTV. He said that third parties, such as police agencies, could request disclosure pursuant to the Privacy Act by submitting a Disclosure of Personal Information Without Consent Form ("Disclosure Request Form"). If a request was approved and submitted to the SOC, he would conduct the search.
- [28] He explained that BPSS is a system deployed by CATSA to validate a passenger's right to access the passenger hold room of an airport. The information captured when a boarding pass is scanned includes the passenger name, air carrier, flight number, departure gate, destination, scheduled departure date, time and seat number.
- [29] On June 14, 2018, Mr. Lalonde received from Darlene Parker, an approved Disclosure Request Form and the pictures of the three men provided by Sgt. Renard. He reviewed the Disclosure Request Form and confirmed that it had been approved.
- [30] Sgt. Renard's request did not include the names of the passengers, just photographs of the individuals in question and flight information. His request included asking if CATSA could identify the individuals in the photographs and locate their flight data. Based on the flight information Sgt. Renard provided, Mr. Lalonde searched the CCTV video of public areas within YOW and located CCTV images that he believed matched the photographs. He was then able to identify the individuals from a BPSS search based on the time of the CCTV. He took still photographs of each individual from the CCTV video and attached them to an

email to Sgt. Renard along with the names and flight information taken from the BPSS.

Francie Lagadyn

- [31] Francie Lagadyn is a security guard for SOC at YVR. In June 2018 her responsibilities included monitoring the alarm system at YVR, monitoring CCTV footage of YVR and dispatching security personal when needed.
- [32] In her affidavit, she deposed that her employer is Securiguard Services LTD. She has never been employed by CATSA.
- [33] She explained that YVR's CCTV footage is available to police and law agencies upon request. A police officer requesting the CCTV footage must complete a request form for the SOC manager's approval.
- [34] In response to Sgt. Renard's request on June 14, 2018, she reviewed the CCTV footage and located individuals arriving on an Air Canada flight from Ottawa that she believed matched the photographs Sgt. Renard had provided. Her SOC manager approved and authorized the release of the CCTV footage to Sgt. Renard. Files were copied to a hard drive and provided to Sgt. Renard.
- [35] She explained that CCTV cameras at YVR are overt, meaning that they may be seen by the public at the airport. There are at least 50 signs both in English and French alerting the public to the presence of the CCTV cameras, which state:
- "This Area is Monitored by Closed Circuit Cameras"; and
 - "Vancouver Airport Authority operates CCTV cameras for safety, security and operational purposes. Information? privacyofficer@yvr.ca".
- [36] The signs are located at most, if not all, entry doors, and in other areas accessible to the public.
- [37] Ms. Lagadyn agreed in cross-examination that the signs do not say that that images will be recorded or that they will be shared with the police. She also agreed that she had to view CCTV images of hundreds of people for this request.

Kelsey MacTavish

- [38] Kelsey MacTavish has been the General Manager, Program Delivery at CATSA since 2013.
- [39] She deposed in her affidavit that CATSA must validate a passenger's need and right to access the passenger hold room of an airport prior to boarding a flight. This is done by verifying the validity of all boarding passes. At Canada's largest airports, this validation occurs through the use of BPSS, which detects fraudulent and duplicate boarding passes. BPSS is also used to determine traffic levels and wait times, to respond to security incidents, and to respond to passenger claims and complaints.

- [40] Where BPSS is used, a boarding pass is scanned twice: first by a CATSA officer when a passenger is in a screening queue, and second by a stationary device prior to the security screening machines, where the results are displayed on a screen visible to a screening officer.
- [41] From scanning a boarding pass, CATSA captures the following information: the passenger's name, the air carrier and flight number, the destination, the scheduled departure date and time, the seat number, the departure gate, and the time and screening line where the boarding pass was scanned.
- [42] The passenger name is retained in CATSA's servers for 30 days, after which it is automatically deleted unless there is a need to retain the data for longer, such as to investigate a security incident, a passenger complaint or claim, a lawsuit, or to respond to a lawful disclosure request from law enforcement or Security agency.
- [43] The passenger's seat number is retained for only 24 hours. Data that is not linked to a specific person may be retained for varying periods, ranging from 3 to 10 years.
- [44] On occasion, CATSA receives requests from law enforcement agencies for information obtained through the BPSS. Such requests must be made through the approved form issued by CATSA.
- [45] Ms. MacTavish testified that pursuant to CATSA's policy, it may provide BBPS data and still images from the CCTV cameras, but a warrant is required to provide video recordings due to concerns with divulging how security screening operates.

III. legislative framework

The Privacy Act

- [46] CATSA operates under the ambit of the federal Privacy Act, R.S.C. 1985, c. P-21, s. 2 of which sets out its purpose:
2. The purpose of this Act is to extend the present laws of Canada that protect the privacy of individuals with respect to personal information about themselves held by a government institution and that provide individuals with a right of access to that information.
- [47] "Personal information" is defined as including "the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual."
- [48] Section 8(1) of the Privacy Act sets out the general rule that personal information under the control of a government institution shall not be disclosed without consent of the individual to whom it relates, subject to certain exceptions. Section 8(2) provides, in part:
- 8 (2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed:

...

- (e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;
- (f) under an agreement or arrangement between the Government of Canada or any of its institutions and the government of a province, the council of the Westbank First Nation, the council of a participating First Nation as defined in subsection 2(1) of the First Nations Jurisdiction over Education in British Columbia Act, the council of a participating First Nation as defined in section 2 of the Anishinabek Nation Education Agreement Act, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation;

[49] As set out in Schedule II of the Privacy Regulations SOR/83-508, s. 8(1)(e) of the Privacy Act applies to the RCMP, but not to the VPD.

[50] Pursuant to a July 27, 1983 agreement between the federal government and the province of British Columbia, s. 8(2)(f) applies to the VPD, thereby permitting disclosure "for the purpose of administering or enforcing any law or carrying out a lawful investigation."

Personal Information Protection and Electronic Documents Act

[51] The Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 ("PIPEDA") applies to the YVR Airport Authority, which uses Securiguard to operate CCTV cameras at YVR. Section 2 of PIPEDA defines "personal information" as "information about an identifiable individual".

[52] Schedule I to PIPEDA is a statement of principles. Clause 4.3 of Schedule I provides:

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

[53] Section 7(2) of PIPEDA provides various qualifications to Clause 4.3. One of the qualifications is as follows:

7 (2) For the purpose of clause 4.3 of Schedule I, and despite the note that accompanies that clause, an organization may, without the knowledge or consent of the individual, use personal information only if;

- (a) in the course of its activities, the organization becomes aware of information that it has reasonable grounds to believe could be useful in the investigation of a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, and the information is used for the purpose of investigating that contravention;...

[54] Section 7(3) also provides for disclosure of information without consent. The relevant portions of s. 7(3) provide:

7(3) For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may disclose personal information without the knowledge or consent of the individual only if the disclosure is

...

- (c) required to comply with a subpoena or warrant issued or an order made by a court, person or body with jurisdiction to compel the production of information, or to comply with rules of court relating to the production of records;

(c.1) made to a government institution or part of a government institution that has made a request for the information, identified its lawful authority to obtain the information and indicated that;

- (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs;

(ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law;

(iii) the disclosure is requested for the purpose of administering any law of Canada or a province, or....

- (d) made on the initiative of the organization to a government institution or a part of a government institution and the organization;

- (i) has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province or a foreign jurisdiction that has been, is being or is about to be committed, or

(ii) suspects that the information relates to national security, the defence of Canada or the conduct of international affairs.

(d.1) made to another organization and is reasonable for the purposes of investigating a breach of an agreement or a contravention of the laws of Canada or a province that has been, is being or is about to be committed and it is reasonable to expect that disclosure with the knowledge or consent of the individual would compromise the investigation;....

IV. policy framework

- [55] The Applicants filed the affidavit of a legal assistant, Alyssa Fazio, attaching some documents that are publicly available on line, including the YVR Airport Authority Privacy Policy, and the CATSA Privacy Policy.

YVR Airport Authority Privacy Policy

- [56] The YVR Airport Authority Privacy Policy sets out, as an "overview", that in order to provide "a safe, secure, and world-class experience, we sometimes need to collect, use and disclose your personal information", which is defined as including, amongst other things, "video surveillance". Personal information may be collected for safety purposes, as well as commercial reasons, such as "direct marketing". The Airport Authority views the use of airport products, services, or facilities as "implying your consent for us to collect, use and disclose your personal information for the purposes set out in this Policy."
- [57] The topic of Video Surveillance is covered on page 6, stating that YVR uses "24-hour video surveillance throughout the airport and the surrounding area", for the purposes of safety, regulatory requirements, and monitoring operations. If one visits the airport, one "cannot refuse to consent to video surveillance." "When you visit any of our premises, including our parking lots and outside areas, you will be recorded and any video surveillance data may be collected, used and disclosed in accordance with this Policy."
- [58] The Policy elaborates that privacy is taken "very seriously" and video is only disclosed "to ensure safe and secure operations at YVR, where we are required by law, or with the consent of the individual who has been recorded."
- [59] Pages 7-8 of the Policy explain that personal information may be disclosed to third parties, including financial institutions, government agencies and security contractors to "facilitate services or ensure the security of our property." The Policy sets out that personal information may be transferred outside of Canada, where different laws may apply.

CATSA Privacy Policy

- [60] The CATSA Privacy Policy provides that CATSA protects personal information in accordance with the Privacy Act, and applicable regulations, policies, directives, and guidelines. The Policy explains why boarding pass information and CCTV video are collected. "Personal information may only be used for identified purposes or consistent purposes as outlined in "InfoSource", and CATSA will only disclose personal information with consent, "or as permitted by the Privacy Act or any other applicable law (e.g. disclosures to law enforcement agencies as per Section 8(2) of the Privacy Act)."
- [61] InfoSource is a document that "provides information about the functions, programs, activities and related information holdings of government institutions."

[62] The InfoSource document describes CATSA Functions, Programs and Activities, and lists the "consistent uses" of information obtained during pre-board screening. The "consistent uses" include disclosure for managerial purposes, security, statistics, and for responding to public complaints. Further, "personal information may be shared with the RCMP or local law enforcement when a passenger is using a fraudulent boarding pass or a security incident has occurred." Personal information "may be disclosed to airport authorities for security purposes." Information about "aviation security incidents" may be disclosed for a variety of purposes, and in particular, "Personal information may be shared with the RCMP, local law enforcement agencies or Transport Canada for incidents suspected to be criminal offences."

V. charter section 8 and the right to privacy

[63] The protection against unreasonable search and seizure is guaranteed under s. 8 of the Canadian Charter of Rights and Freedoms. That section provides:

8. Everyone has the right to be secure against unreasonable search or seizure.

[64] Early in the development of Charter jurisprudence, the Supreme Court of Canada clarified that s. 8 is directed at the protection of people, not places: *Hunter et al. v. Southam Inc.*, [1984] 2 S.C.R. 145. In particular, it is concerned with the protection of a person's reasonable expectation of privacy. As explained by Sopinka J. in *R. v. Plant*, [1993] 3 S.C.R. 281 at para. 16:

The purpose of s. 8 is to protect against intrusion of the state on an individual's privacy. The limits on such state action are determined by balancing the right of citizens to have respected a reasonable expectation of privacy as against the state interest in law enforcement.

[65] The Supreme Court has recognized that the right to privacy is not absolute, but rather must be balanced against society's legitimate concern for protection from crime. The balance is achieved by the qualification that it is reasonable expectations of privacy that are subject to Constitutional protection. As Binnie J. explained in *R. v. Tessling*, [2004] 3 S.C.R. 432 at para. 17:

[17] At the same time, social and economic life creates competing demands. The community wants privacy but it also insists on protection. Safety, security and the suppression of crime are legitimate countervailing concerns. Thus s. 8 of the Charter accepts the validity of reasonable searches and seizures. A balance must be struck, as held in *Hunter v. Southam*, *supra*, at pp. 159-60, per Dickson J.:

... an assessment must be made as to whether in a particular situation the public's interest in being left alone by government must give way to the government's interest in intruding on the individual's privacy in order to advance its goals, notably those of law enforcement.

- [66] The Court in *R. v. Duarte*, [1990] 1 S.C.R. 30 rejected the use of a pure "risk analysis" in determining when an expectation of privacy is reasonable. Although the question of what expectations are reasonable is fact-specific, it also has a normative component, involving an assessment of community values. That normative component was discussed by Doherty J.A. in *R. v. Orlandis-Habsburgo*, 2017 ONCA 649:
- [41] ...the court, in determining whether the claimant has demonstrated a reasonable expectation of privacy, is not engaged in a factual inquiry in the usual sense. The court must, in examining the relevant facts, make a determination that is not purely fact driven, but is also reflective of fundamental societal values. A finding that a claimant has a reasonable expectation of privacy is not only a description of a specific constellation of factual considerations, but is also a declaration of societal aspirations and values. [citations omitted]
- [67] In *Tessling*, at para. 19, the Supreme Court of Canada noted that a principled approach to s. 8 of the Charter requires a consideration of the "totality of the circumstances" with "particular emphasis on (1) the existence of a subjective expectation of privacy; and (2) the objective reasonableness of the expectation".
- [68] The Court went on to distinguish three types of privacy interest protected by s. 8: personal privacy protecting bodily integrity; territorial privacy implicating the places that a person may occupy; and informational privacy, defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others": *Tessling*, at para. 23, quoting A.F. Westin, *Privacy and Freedom* (1970), at p. 7.
- [69] In the present case, the Applicants submit that the primary focus is on informational privacy.
- [70] Not all information is subject to Constitutional protection. In *R. v. Plant*, [1993] 3 S.C.R. 281, for example, the Court held that a warrantless computer search of records of electricity consumption at a residence did not violate s. 8 of the Charter because those records did not disclose intimate details about the accused. Referring to *United States v. Miller*, 425 U.S. 435 (1976), Sopinka J wrote at p. 293:

While I do not wish to be taken as adopting the position that commercial records such as cancelled cheques are not subject to s. 8 protection, I do agree with that aspect of the *Miller* decision which would suggest that in order for constitutional protection to be extended, the information seized must be of a "personal and confidential" nature. In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual. The computer records investigated in the case at bar while revealing the pattern of electricity consumption in the residence cannot reasonably be said to reveal intimate details of

the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence.

[71] Despite the reference to a "biographical core" of information, the Court in *R. v. A.M.*, 2008 SCC 19 noted at para. 68:

Not all information that fails to meet the 'biographical core of personal information' test is thereby open to the police.

[72] Moreover, in *R. v. Tessling* at para. 26, Binnie J. noted that Sopinka J's use in *Plant* of the phrase "intimate details of the lifestyle and personal choices" was not meant to be exhaustive.

VI. application of CHARTER SECTION 8 in previous cases

[73] To illustrate the situations in which s. 8 of the Charter has been applied, the Applicants referred me to several trial rulings.

[74] In *R. v. Flintroy*, 2018 BCSC 1692, the police requested a copy of an individual's passport photograph from Citizenship and Immigration Canada, and it was provided to them without prior judicial authorization. Mr. Justice Williams found that the individual had a reasonable expectation of privacy in his photograph and therefore had standing to challenge the search. In a subsequent ruling, *R. v. Flintroy*, 2018 BCSC 1777, Williams, J. concluded that the search violated s. 8 of the Charter.

[75] In *R. v. Roudiani*, 2018 BCSC 1101, police were investigating an alleged assault that had been captured by security video on the street. The admissibility of the security video was not challenged, but the accused did challenge the admission of a photograph and information collected in connection with a program called BarWatch, where patrons provide their name and submit to being photographed upon entering a nightclub. With this information, the police were able to match the otherwise anonymous video of the assault, with the photograph and name the accused gave upon entering the nightclub. There was no evidence of any notice posted in the nightclub explaining the use to which BarWatch information could be put. N. Smith, J. found that the accused had a sufficient reasonable expectation of privacy in the BarWatch information that its seizure without prior judicial authorization was a violation of his rights under s. 8 of the Charter.

[76] In *R. v. Wong*, 2017 BCSC 306, the accused challenged the admissibility of warrantless video surveillance of activities occurring in the rear driveway and backyard area of a residence. The video camera had been installed by the police on a utility pole. Mr. Justice Kent found that the installation of the camera did not involve a trespass and that the activities captured by the camera would have been plainly visible to anyone observing the scene from the alleyway. Mr. Justice Kent referred to the decision in *R. v. Kwiatkowski*, 2010 BCCA 124, where the British Columbia Court of Appeal found that the warrantless use of an aerial camera and telephoto lens to observe a greenhouse did not violate s. 8 because the observations recorded by the camera were in public view and did not reveal activity taking

place in dwelling houses or other private structures. However, Mr. Justice Kent distinguished that case and found that in the case before him the surveillance violated s. 8 because of the fact that the covert video was continuously recorded for a prolonged period of time and related to the backyard of a private residence. He wrote at para. 47:

- [47] In my view, three weeks of covert 24-hour video surveillance by the police creating a permanent electronic record of activities in the backyard of a private residence is precisely the type of investigative technique that s. 487.01 of the Criminal Code was designed to address. The failure of the police to obtain a general warrant authorizing such surveillance results in a violation of an individual's rights under s. 8 of the Charter.
- [77] More recently, in *R. v. Latimer*, 2020 BCSC 488, Ker J. found that the warrantless seizure of CCTV footage and key fob access records in relation to common areas of two apartment buildings violated s. 8 of the Charter. In coming to that conclusion, she emphasized that the search involved residential premises.
- [78] Crown counsel submits that in relation to the case at bar, the more relevant decisions are those relating to CCTV images recorded in public places.
- [79] For example, in *R. v. Ley and Wiwchar*, 2014 BCSC 2108, Bowden J. held that the accused had no expectation of privacy with respect to his image, posture, gait, clothing, or activities, while in the Edgewater Casino in Vancouver, although he did have a reasonable expectation of privacy in the screen of his Blackberry that was captured by the camera.
- [80] Similarly, in *R. v. Merritt*, 2017 ONSC 366, it was held that a customer had no reasonable expectation of privacy in a video recording of him purchasing shoes in a Walmart store. Dawson J. wrote at paras. 98 and 100:
- [98] Here the video does not show Mr. Fattore doing anything that was of a private or revealing nature. The police were interested in determining whether he bought a pair of shoes and that is what the video shows. The police were not trying to use what can be seen on the video to look inside a more private space, such as a home, hotel room or backpack. Cases like *Wong* and *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 156, are, therefore, distinguishable. The police were interested in finding out what Mr. Fattore did in a large department store on one occasion, openly and in the presence of others.
-
- [100] I do not see that anonymity is of much significance in the circumstances here. This is not a situation like *Spencer* where the police had a significant amount of information about internet activity which revealed a great deal about personal preferences and choices and just needed a link to tie that highly private information to persons who accessed the internet using a particular IP address. As Mr. McGuire put it: "There is no mask of anonymity at Walmart."

[81] In *R. v. Brewster*, 2019 ONCA 942, the Ontario Court of Appeal held that the accused did not have a reasonable expectation of privacy in the underground parking garages of their condominiums. The Court observed at para. 80:

...The appellants had no reasonable expectation of privacy regarding observations made from a space accessible to the general public. Even if the appellants had a subjective expectation of privacy in the garage, that expectation was not objectively reasonable.

[82] In addition to these decisions, the parties have referred me to numerous other trial rulings concerning the application of s. 8 of the Charter, including:

- *R. v. Bryntwick*, [2002] O.J. No. 3618 (SCJ);
- *R. v. Ferguson*, 2018 BCSC 1539;
- *R. v. Flintroy*, 2019 BCSC 213;
- *R. v. Law* (June 12, 2020, Richmond 62633 (BCPC));
- *R. v. Law*, 2017 BCSC 1241;
- *R. v. Piasecki*, 2017 ABQB 192;
- *R. v. Tan*, 2010 BCSC 1948.

[83] I do not find it necessary to summarize each of those cases. While they are illustrative of the application of the relevant legal principles, I must be guided primarily by the jurisprudence from the Supreme Court of Canada and from the British Columbia Court of Appeal. The Supreme Court of Canada has mandated a test based on the "totality of the circumstances", which clearly varies from case to case.

[84] I shall therefore proceed to consider the application of the totality of the circumstances to the case at bar.

VII. the totality of circumstances test in the present case

[85] As set out in *R. v. Cole*, 2012 SCC 53 at para. 40, and more recently in *R. v. Marakah*, 2017 SCC 59 at para. 11, applications under s. 8 of the Charter are to be determined in accordance with the "totality of the circumstances" test, which involves four lines of inquiry:

1. What was the subject matter of the alleged search?
2. Did the claimant have a direct interest in the subject matter?
3. Did the claimant have a subjective expectation of privacy in the subject matter?
4. If so, was the claimant's subjective expectation of privacy objectively reasonable?

Subject Matter of the Search

- [86] In *R. v. Spencer*, 2014 SCC 43, Cromwell J. emphasized that an important first step in any section 8 inquiry is to identify properly the subject matter of the impugned search. As he stated at para. 26:
- [26] ...While, in many cases, defining the subject matter of the search will be uncontroversial, in cases in which it is more difficult, the Court has taken a broad and functional approach to the question, examining the connection between the police investigative technique and the privacy interest at stake. The Court has looked at not only the nature of the precise information sought, but also at the nature of the information that it reveals.
- [87] At para. 31 he added that "the tendency of information sought to support inferences in relation to other personal information must be taken into account in characterizing the subject matter of the search."
- [88] This approach was further explained by McLachlin C.J. in *R. v. Marakah*, at para. 15:
- [15] The subject matter of a search must be defined functionally, not in terms of physical acts, physical space, or modalities of transmission. As Doherty J.A. stated in *R. v. Ward*, 2012 ONCA 660, 112 O.R. (3d) 321, at para. 65, a court identifying the subject matter of a search must not do so "narrowly in terms of the physical acts involved or the physical space invaded, but rather by reference to the nature of the privacy interests potentially compromised by the state action". In *Spencer*, at para. 26, Cromwell J. endorsed these words and added that courts should take "a broad and functional approach to the question, examining the connection between the police investigative technique and the privacy interest at stake" and should look at "not only the nature of the precise information sought, but also at the nature of the information that it reveals". The court's task, as Doherty J.A. put it in *Ward*, is to determine "what the police were really after" (para. 67).
- [89] With these principles in mind, what was the subject matter of the search in the case at bar?
- [90] The Crown submits that with respect to the CCTV video from YVR and the still images at YOW from CATSA, the subject matter of the search was "the physical appearance of the two Applicants in a public place." With respect to the boarding pass information from the BPSS system, the Crown submits the subject matter was "the names and flight details of the two Applicants."
- [91] The Applicants submit that the seizure of the CCTV images and the search of the BPSS data should be considered together and that the subject matter of the search was:

Information about the identifies, associations, and activities of the Applicants as well as recorded video and images depicting their movements in the secure and non-secure areas of Ottawa Airport and YVR, from which the police intended to draw inferences regarding their alleged involvement in criminal activity.

- [92] In my view, applying the broad and functional approach set out in *R. v. Spencer* and *R. v. Marakah*, the subject matter of the search of the CCTV images and still images from YOW and YVR is properly defined as the appearance and movement of the Applicants through the two airports on the date and time in question. Framing it in terms of what the police were really after, the police sought to find out whether, on June 12, 2018, the men depicted in the still photographs that Sgt. Renard supplied to Ms. Lagadyn and to Ms. Parker, had passed through YOW to board a flight to YVR and whether they had passed through YVR after arriving on a flight from YOW to YVR.
- [93] The subject matter of the search of BBPS was the data captured by that system when the Applicants had their boarding passes scanned, namely, their names, the flight they were on, the scheduled departure gate and time, and the time and place each boarding pass was scanned. What the police "were really after" was to attach names to the persons who had been seen in the CCTV images.

Direct Interest

- [94] The second component of the the "totality of the circumstances" test is whether the claimant had a direct interest in the subject matter of the search. In the present case, the Crown concedes that both Applicants did have such a direct interest.

Subjective Expectation of Privacy

- [95] The third line of inquiry in the "totality of the circumstances" test is whether the claimant had a subjective expectation of privacy in the subject matter of the search.
- [96] In the present case, neither of the Applicants adduced any direct evidence, whether by affidavit or viva voce, that they subjectively expected privacy with respect to their movements through the two airports on June 12, 2018 or with respect to their names and flight information captured when their boarding passes were scanned.
- [97] The Crown submits that there has been no demonstrated subjective expectation of privacy.
- [98] The Applicants, however, submit that the subjective expectation of privacy aspect of the test does not pose a high hurdle and that such subjective expectation can be inferred or presumed. They refer to paras. 16-34 of *R. v. Jones*, 2017 SCC 60 for the proposition that they are entitled to rely on the Crown's theory to establish a subjective expectation of privacy.
- [99] I have difficulty appreciating how the principles articulated in *R. v. Jones* assist the Applicants. Even if one accepts the Crown theory that the Applicants are in fact the men depicted in the photographs that Sgt. Renard supplied to Ms. Lagadyn and Ms. Parker, that does not, by itself, support an inference that they subjectively had an expectation of privacy about their flight to Vancouver and their passage through the two airports.

- [100] Although I agree that a subjective expectation of privacy may, in proper circumstances, be inferred from all the evidence, one still must look for a body of evidence from which that inference could be drawn. I have difficulty appreciating what that body of evidence might be in the case at bar. It should be noted that this case is quite different from *R. v. Jones*, where the court inferred a subjective expectation of privacy from the fact that the accused used third-party names so as to avoid detection or association with their text messages. In the present case, there is no evidence that the Applicants took any steps to disguise themselves, or to hide their appearance, or to use false names in connection with their flight from Ottawa to Vancouver.
- [101] At para. 126 of the Applicants' written submission, counsel points to the policy guidelines and legislation as an evidentiary foundation for a subjective expectation of privacy, "whether or not there exists evidence that the applicant in question ever reviewed the same." Such an approach invites the question, in what sense is such an expectation "subjective", if it is divorced from the facts relating to the particular rights claimant?
- [102] In the end, it appears that the Applicants' argument is that anyone flying between major airports in Canada would naturally expect to have privacy with respect to their travel, which amounts to saying that an expectation of privacy would be reasonable in the circumstances. But to base a subjective expectation of privacy on the notion that such an expectation would be objectively reasonable for anyone in the circumstances, is simply to collapse the third and fourth lines of inquiry into one.
- [103] Nevertheless, I recognize that the cases have tended to put little emphasis on the subjective expectation of privacy component of the totality of the circumstances test. For example, in *R. v. Jones* at para. 21, the Court emphasized that the normative import of s. 8 transcends the individual's expectations:
- [21] The idea here is simple: a Charter claimant's subjective belief that Big Brother is watching should not, through the workings of s. 8, be permitted to become a self-fulfilling prophecy. The importance of the subjective expectation element is therefore attenuated in the s. 8 analysis, and the evidentiary foundation required to establish that element is accordingly modest. A subjective expectation of privacy can be presumed or inferred in the circumstances in the absence of the claimant's testimony or admission at the voir dire (see *Patrick*, at para. 37; *Tessling*, at para. 38; *Cole*, at para. 43). The modest evidentiary foundation necessary to establish one's subjective expectation of privacy therefore reflects the notion that s. 8's normative import transcends an individual claimant's subjective expectations.
- [104] And in *Tessling*, at para. 42, the Court appears to have held that s. 8 protection may be found even in a case where the subjective expectation of privacy is absent:
- [42] I should add a caveat. The subjective expectation of privacy is important but its absence should not be used too quickly to undermine the protection afforded by s. 8 to the values of a free and democratic society. In an age of expanding means for snooping readily available on

the retail market, ordinary people may come to fear (with or without justification) that their telephones are wiretapped or their private correspondence is being read. One recalls the evidence at the Watergate inquiry of conspirator Gordon Liddy who testified that he regularly cranked up the volume of his portable radio to mask (or drown out) private conversations because he feared being "bugged" by unknown forces. Whether or not he was justified in doing so, we should not wish on ourselves such an environment. Suggestions that a diminished subjective expectation of privacy should automatically result in a lowering of constitutional protection should therefore be opposed. It is one thing to say that a person who puts out the garbage has no reasonable expectation of privacy in it. It is quite another to say that someone who fears their telephone is bugged no longer has a subjective expectation of privacy and thereby forfeits the protection of s. 8. Expectation of privacy is a normative rather than a descriptive standard.

[105] For this reason, I agree with the Applicants that the present case should not be decided on the basis of whether or not they had a subjective expectation of privacy.

Objectively Reasonable Expectation of Privacy

[106] We come then, to the fourth line of inquiry: was an expectation of privacy objectively reasonable in the circumstances? All parties agree that this question is at the heart of this s. 8 inquiry.

[107] In *R. v. Tessling*, at para. 32, the Court enumerated seven factors that may usefully be examined in determining whether an expectation of privacy was reasonable in all the circumstances. These were conveniently restated by Ker J. in *R. v. Latimer*, at para. 194:

- a. The place where the alleged "search" occurred; in particular, did the police trespass on the applicant's property and, if so, what is the impact of such a finding on the privacy analysis?
 - b. Whether the informational content of the subject matter was in public view.
 - c. Whether the informational content had been abandoned.
 - d. Whether such information was already in the hands of third parties; if so, was it subject to an obligation of confidentiality?
 - e. Whether the police technique was intrusive in relation to the privacy interest.
 - f. Whether the use of this evidence gathering technique was itself objectively unreasonable.
 - g. Whether the informational content exposed details of the claimant's lifestyle, or information of a biographical nature.
- (a) The Place where the Search Occurred

- [108] In the case at bar, the search occurred in those areas of YOW and of YVR that passengers routinely pass through when boarding or arriving from a commercial airline flight. It was there that the images in question were captured, and it was there that the Applicants presented their boarding passes as a part of the normal routine of travelling on a commercial airline flight in Canada. The place of the search was a public place.
- [109] I do not accept the Applicants' submission at para. 147 of their submissions, that what the police sought was not in a public place because "it was carefully safeguarded in electronic databases" that were "physically secured and electronically encrypted." In effect, it appears that the Applicants' position is that the place of the search should be defined as the computers or other electronic devices where the images and boarding pass data were stored in electronic form. In support of this submission, they refer to *R. v. Marakah*, at para. 27:
- [27] The factor of "place" was largely developed in the context of territorial privacy interests, and digital subject matter, such as an electronic conversation, does not fit easily within the strictures set out by the jurisprudence. What is the place of an electronic text message conversation? And what light does that shed on a claimant's reasonable expectation of privacy? Place is important only insofar as it informs the objective reasonableness of a subjective expectation of privacy.
- [110] The Court in *R. v. Marakah* was grappling with the question of how to describe the "place" of an electronic conversation. The court recognized that the seizure of electronic communications is different from other kinds of seizures or observations, and in that context, the question of "place" may be of little analytical utility.
- [111] It would be a mistake, however, to treat *R. v. Marakah* as establishing a new paradigm for the role of "place" in a s. 8 analysis. The present case has nothing to do with electronic conversations, and the analysis of "place" in *R. v. Marakah* has little relevance to the present context.
- [112] Rather, the description of "place" in the case at bar should follow an analysis similar to that in *R. v. Tessling*. There, the Court had to consider heat-sensing technology called "FLIR" that had been used to observe the amount of heat emanating from the roof of a building. At para. 45, the Court described the place searched as the "exterior of the respondent's home". Notably, this description of place had nothing to do with the internal technical workings of the FLIR apparatus. Rather, the "place" was defined in terms of the physical location that the FLIR equipment was used to observe.
- [113] Just as in *R. v. Tessling*, the primary focus should be on what was being observed, not the technological details of the equipment used to make or store the observations.

[114] The observations here were in a public place - an airport. The observations did not involve any trespass on the Applicants' property. The relevant description of the place is not affected by the fact that the images or data were stored in electronic form on a computer with limited access.

(b) Was the Informational Content in Public View?

[115] The Applicants chose to pass through both YOW and YVR without disguising their appearance or otherwise hiding their identity. They were there for anyone to see, and indeed, were no doubt observed by dozens, if not hundreds of persons. The fact of their passing through both airports is a matter that was on public view.

[116] As Binnie, J. observed in *R. v. Tessling* at para. 40:

[40] It is true that a person can have no reasonable expectation of privacy in what he or she knowingly exposes to the public, or to a section of the public, or abandons in a public place.

[citations omitted]

[117] As for the boarding pass data from the BPSS system, most of this information was also open to public view, in the sense that anyone in the relevant parts of the airports could see what the Applicants' departure gate was at YOW and what their arrival gate was at YVR. The flight number and departure and arrival times would no doubt have been posted on publically visible Arrivals and Departures screens.

(c) Had the Informational Content Been Abandoned?

[118] The issue of whether seized material had been abandoned is an important part of the analysis in cases where a person has discarded a used tissue or thrown out papers in the garbage, but it has little relevance to the case at bar. In the present case, this is a neutral factor.

(d) Was the Information in the Hands of Third Parties and Was it Subject to an Obligation of Confidentiality?

[119] In the case at bar, the information was in the possession of CATSA, but there was no contract between CATSA and the Applicants.

[120] I do not agree with the Applicants' submission at para. 196 of their written argument that "although the subject matter of this search was in the possession of the Vancouver Airport Authority and CATSA, those authorities were bound to maintain the confidentiality of that information vis a vis law enforcement, unless disclosure related specifically to airport or air transport related issues."

[121] The CATSA Privacy Policy advises the public that it may disclose information to law enforcement agencies pursuant to s. 8(2) of the Privacy Act. As set out above, the combined effect of the July 27, 1983 agreement between the federal government and the province of British Columbia and s. 8(2)(f) of the Privacy Act is to permit disclosure to the VPD "for the purpose of administering or enforcing any law or carrying out a lawful investigation."

[122] In the end, I come to the same conclusion as the Court did in *R. v. Spencer*, namely that a consideration of the legislation and the policy statements, while providing necessary background and context, do not ultimately answer the question of whether there was a reasonable expectation of privacy, since their application depends on an understanding of what the police were lawfully entitled to do, and that in turn, depends on whether their search violated s. 8 of the Charter. As Cromwell J. expressed it at para. 61 of *R. v. Spencer*:

The provisions of PIPEDA are not of much help in determining whether there is a reasonable expectation of privacy in this case. They lead us in a circle.

(e) Was the Police Technique Intrusive in Relation to the Privacy Interest?

[123] The technique employed by the police in this case involved making written requests for information about the three men. The requests were not wide-ranging; they did not seek a review of CCTV footage over a period of days or of multitudinous public places. On the contrary, the request particularized a specific date and time, and mentioned two specific flight numbers at two specific airports. The request was accompanied by photographs of the three men who were being sought. This narrow focus supports the conclusion that the police technique was not intrusive.

(f) Was the Use of This Evidence Gathering Technique Objectively Unreasonable?

[124] For similar reasons, I find that there was nothing objectively unreasonable about this technique.

[125] The Applicants referred to the discussion of "privacy as anonymity" in *R. v. Spencer* and submit that they had a right to anonymity at the two airports, despite the fact that they are public places. One must not lose sight, however, of the context in which anonymity was discussed in *R. v. Spencer*. There, the issue was privacy with respect to internet activity, which the Court found to "engage a high level of informational privacy."

[126] I agree with the Crown's submission that a fair reading of paragraphs 38-51 of *R. v. Spencer* shows that the Court was not there advancing a general principle that every identification of a person in public engages the protections of s. 8. Rather, the examples discussed in *R. v. Spencer* at paras. 42-44 show that the Court's concern was with overly intensive or ubiquitous monitoring.

[127] In the case at bar, the police inquiry was focused and limited with respect to both time and place. It was not objectively unreasonable.

(9) Did the Informational Content Expose Details of the Claimant's Lifestyle, or Information of a Biographical Nature?

[128] Thousands of people pass through Canada's airports every day. The routine nature of such an event suggests that in most cases, the fact of passing through an airport reveals very little about a person's lifestyle and does not expose information of a biographical nature. In the case of the two Applicants in the case at bar, there was nothing extraordinary about their passage through YOW and YVR; nothing that would set them apart from the thousands of other people using that public space. Although the images show the three men apparently together, there would be nothing unusual or particularly revealing about that. People routinely travel in groups of two or three. In short, the CCTV and still photos do not expose details of the Applicants' lifestyle or information of a biographical nature.

[129] The same is true with respect to the data from their boarding passes, with the possible exception of their names. As the Applicants point out at para. 157 of their argument, "Their names were not available to the public at large as they walked through Ottawa and Vancouver airports".

[130] Nevertheless, I agree with the Crown's submission that there is no freestanding right to have one's name kept private, and that Constitutional protection is not necessarily extended to every piece of information an individual may wish to keep confidential. As Binnie J. noted in *R. v. Tessling* at paras. 25-26:

[25] Privacy is a protean concept, and the difficult issue is where the "reasonableness" line should be drawn. Sopinka J. offered a response to this question in the context of informational privacy in *Plant*, *supra*, at p. 293, as follows:

In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual. [Emphasis added]

[26] I emphasize the word "include" because Sopinka J. was clear that his illustration ("intimate details of the lifestyle and personal choices") was not meant to be exhaustive, and should not be treated as such. Nevertheless, *Plant* clearly establishes that not all information an individual may wish to keep confidential necessarily enjoys s. 8 protection.

[131] The jurisprudence provides many examples of cases in which no reasonable expectation of privacy was found with respect to the name provided by a passenger in connection with boarding a commercial air flight.

[132] In *R. v. Chehil*, 2009 NSCA 111, the police obtained, without warrant, the passenger manifest for a WestJet flight, and discovered the information that was entered when the accused purchased his ticket, including his name and the flight details. That information was subject to PIPEDA. The Nova Scotia Court of Appeal found that this information did not

engage either the accused's subjective expectation of privacy or an objectively reasonable expectation of privacy. The Court noted at para. 42 that although the electronic records themselves were not in public view, the accused's actions in buying the ticket, checking his bag, and boarding the flight were all conducted in public.

- [133] In *R. v. Devloo*, 2015 ABQB 345, the police obtained, without a warrant, information from WestJet including the name and basic flight details of a passenger. It was held that there was no reasonable expectation of privacy in this information as the passenger's actions in taking the flight were publicly observable and the flight details were not of an intimate or personal nature. As set out at para 205:
- [205] In this case, the information disclosed did nothing more than expose Mr. Devloo's record of his transactions with WestJet. Unlike an IP address, flight information does not provide a direct route to biographical core information. The ticketing information does not reveal specific nor meaningful information that reveal intimate details of his lifestyle or personal choices.
- [134] In *R. v. Baldovi*, 2016 MBQB 221, the police obtained, without warrant, data from CATSA and WestJet about certain domestic flights on certain dates, plus a photo of the accused passing through security. The Court found no objectively reasonable expectation of privacy, noting that the information arose from activities occurring in public. The search did not expose any intimate lifestyle details and was not biographical in nature.
- [135] Accordingly, in all the circumstances of the present case, obtaining the name that the Applicants used on their boarding passes did not amount to disclosure of information of a core biographical or intimate nature. It did not reveal details of the Applicants' lifestyle. The general truism that starting with a person's name, anyone can try to find out other information about that person, does not affect the reasonableness of Sgt. Renard's very limited request for information from the BPSS system in the present case.

VIII. conclusion

- [136] Applying the totality of circumstances test, and considering the seven factors enumerated at para. 32 of *R. v. Tessling*, I am satisfied that there was no reasonable expectation of privacy in the information obtained by Sgt. Renard in this case. His obtaining of that information without prior judicial authorization did not infringe the s. 8 Charter rights of either of the Applicants.

- [137] Accordingly, the application is dismissed.

"Ehrcke, J."

Source & reproduction note

Judgment wording, source notices and original paragraph numbers are retained. Esheria supplies the layout and this PDF's page numbers; these are not the source pagination. This is a research copy, not an official or certified court document. Check quotations, citations and publication restrictions against the original source before relying on it.

ORIGINAL SOURCE <https://www.bccourts.ca/jdb-txt/sc/20/13/2020BCSC1309.htm>

CASE PAGE <https://chat.esheria.ai/case-law/canada/r-v-ali-boparai-and-malonga-massamba-2020-bcsc-1309>

Prepared on 26 October 2026 · Esheria