Citation: *R. v. Cafferata*, 2008 YKTC 93

Date: 20081219
Docket: 07-00363
Registry: Whitehorse

IN THE TERRITORIAL COURT OF YUKON
Before: His Honour Judge Cozens

R e g i n a

v.

John Cafferata

Appearances:
David McWhinnie — Counsel for Crown
Keith Parkkari — Counsel for Defence

RULING ON VOIR DIRE

Overview

[1] The accused, John Cafferata, is charged with possession of child pornography and accessing child pornography, contrary to ss. 163.1(4) and 163.1(4.1) of the *Criminal Code of Canada*.

[2] An international child pornography investigation in the United States of America with collateral Canadian involvement, known as Project Emissary, identified a number of individuals in Canada who apparently subscribed, or attempted to subscribe, to child pornography websites. Mr. Cafferata was identified as one of these individuals.

[3] The US authorities provided some information about the nature and extent of the US investigation, including the identified Canadian individuals, to the National Child Exploitation Coordination Centre in Ottawa (NCECC). NCECC personnel then provided the RCMP in the Yukon with an information package

concerning Mr. Cafferata. After further investigation by the RCMP in the Yukon, a Production Order was obtained on June 14, 2007 for Mr. Cafferata's Visa records. After receiving and reviewing these records, the RCMP obtained a Search Warrant on August 28, 2007 to search the home, vehicle and outbuildings of Mr. Cafferata.

Issues

[4] Counsel for Mr. Cafferata asks that the Production Order and Search Warrant be declared unconstitutional as being unreasonable search and seizures contrary to Mr. Cafferata's rights under s. 8 of the *Charter*, and that the evidence obtained as a result of these searches be excluded under s. 24(2). Broadly speaking, defence counsel's position is that portions of the affidavit relied upon in the application for the Production Order (the "Affidavit") were inaccurate and misleading and, as such, upon review and amplification at trial, there is insufficient evidence to find that the justice who issued the Production Order could have done so.

[5] As such, he argues, the banking records obtained through the Production Order should be excluded from the Information to Obtain ("ITO") that was relied upon in the application for the Search Warrant. After excising these banking records from the ITO, the same concerns about inaccurate and misleading portions of the Affidavit apply to the ITO and, as such, there is insufficient evidence to find that the judge who issued the search warrant could have done so.

[6] Crown counsel concedes that if the Production Order is found to be an unreasonable search and seizure and the banking records expunged from the ITO, then the Search Warrant cannot stand.

[7] Crown counsel also concedes that, if there has been an unreasonable search and seizure, the evidence obtained as a result of the execution of the

Production Order and the Search Warrant would not be admissible under s. 24(2) of the *Charter*.

Evidence

[8] A *voir dire* was entered into at the commencement of the trial to deal with the s. 8 *Charter* challenge to the validity of the Production Order and the Search Warrant. Sgt. Bob Johnson was the sole witness for the Crown on the *voir dire*. Sgt. Johnson had approximately 16 to 17 years of experience as an RCMP officer at the time he received the information about Mr. Cafferata from the NCECC. He was working out of the Major Crimes Unit in Whitehorse. He had some prior, albeit limited, experience in the investigation of computer generated child pornography.

[9] Sgt. Johnson testified that in drafting the sections of the Affidavit and the ITO, he relied upon what he learned from the Department of Homeland Security and the NCECC. He used his language, RCMP Sgt. Peter Payne's, who was on assignment to the Major Case Unit at the NCECC, and that of other individuals. Much was his own writing. He researched his own definitions for the definitions sections of the Affidavit and ITO. He used a precedent binder, but he did not recall cutting and pasting *per se*.

Receipt of Information

[10] In April, 2007 the NCECC sent the information package regarding Mr. Cafferata to the RCMP. Sgt. Johnson reviewed this information package on May 2, 2007.

[11] On May 3, 2007, Sgt. Johnson received a report from Sgt. Payne. Sgt. Johnson confirmed the information in this report with Susan Commance, also employed with the NCECC. He learned the following information:

9. *(both in the Affidavit and ITO)*

…

a. On April 3rd, 2007, Sergeant Peter Payne and Susan Commance both of the NCECC met Department of Homeland Security Special Investigators, Victoria Beechina and Mike Riccitelli of Newark, New Jersey, USA. The purpose of this visit was to clarify vast amounts of information on Project Emissary. The NCECC had received an investigational package on Project Emissary several months previous;

b. over the course of 60 days, the webpage to subscribe for Child Pornography had 84 different URL's (the address used to access the site). Not all of the URL's were captured as they were changing daily. 35 of the URL's were captured for 84 of the Canadian targets. The URL's would contain one or more of the following advertising banners:

    1. Illegal.cp
    2. The Sick Child room
    3. P.T.H.C. XXX A.R.C.H.I.V.E.
    4. Children Porno Portal
    5. Real Child Porno….

Sgt Johnson testified that he could not confirm that Mr. Cafferata ever did anything with these particular sites or saw advertising banners. He assumes that Mr. Cafferata provided information to a join page through some referrer site. He agrees that the ITO does not indicate that Mr. Cafferata was, in fact, not ever actually linked to any of these sites.

…

c. Once a subscriber submitted their completed joining page, they would receive a confirmation e-mail within 24 hours confirming their authorization and approval to enter the site. This e-mail would contain the login, password and URL for the site. The very first screen that would pop up when they entered their user name and password was titled, "FAQ Please Read" and that document guaranteed a reply to the subscribers e-mail within 24 hours. The document also stated that "Our site is considered to be illegal in all countries". It provided further information on problems concerning the police and credit cards; (See Appendix "A" for a sample of a "join page" format and see Appendix "B" for a copy of the pop up warning screen titled "FAQ Please Read this document)

Sgt. Johnson testified that he assumed the response would be by electronic e-mail. He could not say whether all e-mails, outgoing and incoming would have been intercepted by the US investigative authorities.

…

d. There are four sites which subscribers used to access child pornography and each of these URL's or links transferred you to the same child pornography content;

    1. http ://hualama.cjb.net
    2. http ://fargo.sel.to
    3. http ://mhumbu.badlink.net
    4. http ://pliac.hotfire.net

Sgt Johnson testified that these are for general information only, to show how the process worked and not to infer Mr. Cafferata went to any of them. He was told by Sgt. Payne and Susan Commance that these are child pornography sites.

…

e. all of the credit card transactions were processed through JetPay. JetPay is the third largest credit card company authorizer in the world and their address is in Carrollton, Texas, USA;

f. the subscription date could have preceded the message number date by a few days. In this case the message number indicates January 4th, 2006.

g. the information on the subscriber's credit card statement would show a payment made to "Adsoft" for $79.99. Adsoft is a front company for the criminal organization administering access to these child pornography websites.

Sgt. Johnson testified that the Adsoft name was not initially provided by the Department of Homeland Security to the NCECC, but only to Sgt. Payne and Susanne Commance after they met with US officials. They in turn passed this information on to Sgt. Johnson.

…

h. The following HTTP's are the ones that were captured for all of the Canadian targets:

HTTP_REFERERS
Unique sites accessed, as per CANADA.xls

http ://batalyos.net/j.html
http ://bawygowymelou.com/12121/join.html
http ://dynorosy.net/j.html
http ://jkotdsrsea.szm.sk/str/join2.html
http ://kobolt.biz/j.html
http ://lmiok.com/join.html
http ://losita.net/j.html
http ://ragester.net/j.html
http ://shockkoo.100free.com/str/join2.html
http ://thoriuma.net/j.html
http ://udwowbakuwloc.com/access/members.htm
http ://www.primelolitas.com/secure/join_8391.html
http ://www.skladytsi.net/devis/access/members.htm
http ://www.uspasrt.net/join.html
*not all the HTTP referrer sites were captured for every suspect which was the case with CAFFERATA.

Sgt. Johnson testified that of the 83 identified Canadians, 19 had a referer site related to one of these. Sgt. Johnson testified that there was no information captured to indicate that Mr. Cafferata had ever gone to one of these HTTP referer sites. The intercepts only captured subscriber information but no referer site for Mr. Cafferata. Sgt. Johnson could not say whether a member of the public could accidentally access one of these referer sites. He agreed that the Affidavit and ITO could have stated that “none” of the referer sites were traceable to Mr. Cafferata.

[12] Sgt. Johnson reviewed the report provided by the Department of Homeland Security to the NCECC that contained the background information to Project Emissary. He confirmed the information in this report very early on, in perhaps May, 2007, as he testified to in cross-examination, through a telephone call he initiated with Sgt. Mike Riccitelli. Sgt. Riccitelli is a Senior Special Agent with the Department of Homeland Security, Immigration and Customs Enforcement (“ICE”), and a Computer Forensic Agent assigned to the Cyber Crimes Group of the Child Exploitation Unit at the Special Agent in Charge office in Newark, New Jersey. Sgt. Riccitelli assisted in gathering and compiling the

information for distribution and assisted with the computer forensics for Project Emissary.

[13] As a result of reviewing this report and his discussion with Sgt. Riccitelli, Sgt. Johnson became aware of the following information:

> 8. *(both in the Affidavit and ITO*)
> …
> a. After making undercover purchases, executing search warrants, and receiving other evidence, Special Agent in Charge (SAC) Newark's (New Jersey) Child Exploitation Group and Forensic Analysis Group acquired a title III court order. The Title III electronic intercept in the US is equivalent to our Part VI authorizations in Canada.
>
> b. the Title III intercept began on December 27th, 2005 and ended on February 25th, 2006. Over 1500 applications to pay for these child pornography sites were intercepted. The applications contained extensive identifying data on the applicants and many of the applicants were from outside the United States, including Canada;
>
> c. e-mails intercepted during the sixty day intercept of the e-mail account contained ordering information for individuals. The ordering information contained the following for each: login, password, first name, last name, address, city, state/province/territory, zip/postal code, country, e-mail, phone number, credit card number, cvv2, bank name, customer service, card expiration month and year and almost always contained the amount of $79.99 (US funds);
>
> d. the information was provided to agencies outside of the United States also in Spreadsheet format and also a copy of the content of the pornographic Websites;
>
> e. content of the pornographic sites accessed is disturbing in that some of it involves pre-pubescent and very young children engaged in sexual acts, sometimes set in physically abusive scenarios.

Sgt Johnson testified at one point that child pornography was not intermingled with adult pornography on the sites.

[14] Sgt. Johnson reviewed three spreadsheet summaries which he testified he believed he was told by Daniel Lacroix, who is an intelligence analyst with the NCECC, were provided by the Department of Homeland Security.

Canada.xls spreadsheet

[15] The first of these spreadsheets, Canada.xls, was not set out in the Affidavit and ITO. It provided personal information regarding all the Canadian individuals caught in the Title III intercepts.

Canadian Subscribers.xls spreadsheet

[16] The second spreadsheet, included as paragraph 11(a) in the Affidavit and ITO, is identified as Canadian Subscribers.xls. This spreadsheet pertained only to Mr. Cafferata.

[17] The information in this spreadsheet would have been captured during the intercepts and was added to the subscription join page by the purchaser. I note at this point that there is only one Title III intercept identified in the Affidavit and the ITO, being from December 27, 2005 to February 25, 2006. In fact, Sgt. Johnson testified that there were two 30 day Title III intercepts within this period, one from December 27, 2005 to January 25, 2006 and the second from January 27 to February 25, 2006. As such, the reference to “intercepts” in paragraph 11 must be to either these two separate Title III intercepts, or to the various e-mails “intercepted” within the earlier Title III intercept, given the dates set out in the charging Information.

[18] This spreadsheet had a T# message number date of January 4, 2006. Sgt. Johnson testified that he learned from Sgt. Riccitelli only in the 1 – 1 ½ days before trial that the message number was added by the Department of Homeland Security, after the intercept and after analyzing the dates, in order to assist in their investigation. Sgt. Johnson had previously thought that this date had been

caught in the intercept as well. He assumes that the date came from the intercept but he does not know how the US authorities came up with it.

[19] This spreadsheet contained a login of “knobah”, the name of John Cafferata, a Teslin Yukon address of 45 cotlots with (CDN) zip code, a Northwestel e-mail address, a Teslin telephone number, a CIBC credit card number with cvv number and expiry date, a $79.99 (20) transaction and an IP address. It stated “nothing” regarding the sysdata date, time or Http_referer. Sgt. Johnson testified that he had been advised that the T/sysdata date on the Canadian Subscribers.xls spreadsheet could allow for a determination of the date of the transaction between the purchaser, Mr. Cafferata, and the seller. There was no information in the Affidavit or the ITO providing any explanation for why “nothing” was registered in relation to the Sysdata date.

[20] The only difference in the information pertaining to Mr. Cafferata between the Canada.xls and Canadian Subscribers.xls spreadsheets is the inclusion of the T# message number in the latter.

[21] Sgt. Johnson agreed in testimony that for legal purchases over the internet, a purchaser would provide essentially the same information such as name, e-mail address, credit card number with three digit cvv code, shipping and billing addresses.

Canadian Adsoft Transactions.xls spreadsheet

[22] The third spreadsheet, included as paragraph 11(b) in the Affidavit and ITO, was identified as Canadian Adsoft Transactions.xls. This spreadsheet also pertained only to Mr. Cafferata. As contrasted to the Canadian Subscribers.xls spreadsheet in paragraph 11(a), which shows information from Mr. Cafferata by e-mail, providing information for subscription purposes to a child pornography website or account, through, as I understand it, an intermediary account, the Canadian Adsoft Transactions.xls spreadsheet is information received from the

child pornography website or account back to the intermediary account, approving the subscription application. The intermediary account would then, as part of the process, send a confirmatory e-mail with login and password to Mr. Cafferata.

[23] In the Affidavit and the ITO it was stated that the data in this third spreadsheet would have been captured during the intercepts, which as I have stated earlier likely referred to the various e-mails intercepted in the Title III intercept from December 27, 2005 to January 25, 2006, and that the information was added to the subscription join page by the purchaser.

[24] Sgt. Johnson's evidence in the *voir dire* was that when he was reviewing the file just prior to trial, in preparation for testifying, he became concerned about the "C/ transactiondat: 20060429101656" reference in the Canadian Adsoft Transaction.xls spreadsheet. He contacted Sgt. Riccitelli and learned that the information in this spreadsheet was not related to the December 27, 2005 to January 25, 2006 Title III intercept. Sgt. Riccitelli told him that this information was information related to Adsoft that came from follow up search warrants and intercepts throughout their investigation, and this particular spreadsheet related to an Adsoft transaction of $79.99 from April, 2006. Sgt. Johnson cannot be 100% sure which particular follow-up search warrant and intercept it came from or for which company, although he believes it may have been related to JetPay, but cannot say so with certainty.

[25] Sgt. Johnson agreed in his testimony that the ITO and Affidavit, outside of paragraph 11(b) did not contain any information as to whether Mr. Cafferata did or did not receive an e-mail confirmation back in response to a subscription application.

[26] In this sense, his information differed from that originally believed and proffered to the Justice of the Peace who authorized the Production Order and

the Judge who issued the subsequent Search Warrant. The impact of this factor will be discussed later in this ruling.

[27] The third spreadsheet had a transaction id date of April 29, 2006. It also contained the same address and credit card number as the Canadian Subscriber.xls spreadsheet, the cardholder name of "John Cafferata", an amount of $79.9[sic], an order number and an "auth_c" number.

[28] On May 7, 2007, Sgt. Johnson completed a PIPEDA request to Internet Service Provider NorthwesTel of Whitehorse, seeking disclosure of customer identifying information for the IP address in the spreadsheets, for the period of January 1 to 15, 2006.

[29] On May 7 and 10, 2007, Sgt. Johnson reviewed two compact discs (cds) provided to him by the NCECC The cds contained:

> 13. (*both in the Affidavit and ITO*)
> …
> a. The sample join page for subscribing (See Appendix "A");
>
> b. The pop up window screen titled "FAQ Please read" (See Appendix "B");
>
> *c.* The subscriber join capture for jc@northwestel.net (See Appendix "C")
>
> I note that when compared to the Canadian Subscribers.xls spreadsheet, they both contain almost identical information except for "country: canada" in the spreadsheet and "country: CA" in the Appendix; "cvv 214" in the spreadsheet and" cvv: 241" in the Appendix. This would appear to be a typographical error, likely made in the ITO.
>
> Sgt. Johnson testified that he could not explain where Appendix "C" came from other than to state he believes it came from the intercept.
> …

d. numerous disturbing photos and videos of prepubescent children engaging in sexual acts and poses, some with adults. These are the images and files that were accessible to subscribers.

[30] On May 7, 2007, RCMP Corporal Mark Groves confirmed that a vehicle bearing the license plate "Knobah" was parked in the driveway of 45 Cottage Lots in Teslin, Yukon. Cpl. Groves had observed this vehicle at the same residence for approximately the past three years and believed it to be Mr. Cafferata's residence. A 2002 "Report of the Properties of Teslin Cottage Subdivision" provided by Cpl. Groves listed 45 Cottage Lots as the residence of Mr. Cafferata.

[31] On May 10, 2007 Sgt. Johnson conducted a database check with the Yukon Motor Vehicles Branch and found that the driver's license for Mr. Cafferata referenced an address of 4-5 Cottage Lots. He testified that he believes this "4-5", rather than "45", to be a mistake.

[32] On May 8, 2007, Sgt. Johnson reviewed an intelligence summary from the NCECC's review of the Department of Homeland Security investigation, and confirmed the information in this report with Daniel Lacroix. Sgt. Johnson learned the following from the summary and confirmation of the information:

10. *(both in the Affidavit and ITO)*
…

a. the report outlines the name of John Cafferata, his address, phone, E-mail, IP address and credit card information, plus the message number that was generated from the Department of Homeland Security intercept;

b. according to a "Canada 411" internet search conducted by NCECC, the phone comes back to a "landline" in Teslin, Yukon;

c. the IP address in the Cafferata transaction/subscriber data resolves to NorthwesTel Inc., in Whitehorse, Yukon;

> Sgt. Johnson testified that he cannot say how this was determined for the purpose of the report he received, but only that this information was given to him.
>
> …
>
> d. John CAFFERATA has no indication of a formal criminal history or record.

[33] On May 18, 2007 Sgt. Johnson learned that the PIPEDA request for NorthwesTel had confirmed that the identified IP address listed Mr. Cafferata as the customer for January 1-15, 2006. This is the only information contained in paragraph 17 of the Affidavit, which is expanded upon in the same paragraph in the ITO. In a conversation between Sgt. Johnson and NorthwesTel personnel on August 27, 2007, Sgt. Johnson further learned that the following information was associated to Mr. Cafferata and this IP address, and this additional information was added to the ITO:

- Jon Cafferata *(I note not spelled "John" as in other places)*
- L45 Cottage Lots
- Teslin, YT
- P.O. Box 160 Stn. Main
- Teslin Y1A 1B0 *(I note not "Y0A 1B0" as in the spreadsheets and Appendix "C")*
- Phone number: 867-390-2345 *(I note not "867-390-1414" as in the Canadian Subscribers.xls spreadsheet and Appendix "C").*

[34] On June 6, 2007, Cst. Andrew Bechtel confirmed certain information with Cpl. Douglas Wattie, a member of the RCMP Integrated Child Exploitation Section in Calgary, Alberta. Cpl. Wattie offered his opinion that: "His experience is that persons who have downloaded child pornography do tend to keep it because of the risks and difficulty involved in obtaining it". Cpl. Wattie's experience in numerous investigations has been that foreign agencies would forward customer lists containing credit card and IP address information to enforcement agencies in Canada, and the Canadian enforcement agencies would conduct confirmatory investigations and obtain search warrants. The

execution of these warrants would, in the overwhelming majority of cases, locate child pornography in the possession of the subject of the warrant, even after the passage of several years.

Production Order

[35] Based upon the information he had learned, Sgt. Johnson believed that the Canadian Imperial Bank of Commerce ("CIBC") in Whitehorse would possess credit card documentation for Mr. Cafferata that would "…provide evidence to support the subscription and transaction to the child pornography sites and allow police to further their investigation in the search for further evidence of child pornography and exploitation". Sgt. Johnson testified that at this point in the investigation he did not have an Adsoft connection but he expected to find it.

[36] Based upon all the information provided to Sgt. Johnson and relayed to Cst. Andrew Bechtel, Cst. Bechtel swore the Affidavit to obtain the Production Order for the banking documents of Mr. Cafferata in the possession of CIBC.

[37] On July 23, 2007, Cst. Derek Turner seized the documents from the CIBC. These are located in Appendix "D" of the ITO. Sgt. Johnson reviewed these documents and learned the following, as set out in paragraph 21 of the ITO:

> …
>
> a. The customer general information associated to John Cafferata shows an address to PO Box 160 in Teslin, Yukon. The home phone listed is not in Teslin, yet the business number for J. Cafferata is associated to the Teslin School, Cafferata's place of employment. The date of birth listed is February 20, 1953;
>
> b. the Visa Account statements are in the name J. Cafferata and they are linked to credit card number 4500 6214 4636 3012. Transactions made between December 30, 2006 and February 27, 2006 are noted. *(I consider the December, 2006 date to be a typographical error in the ITO and an actual reference to a December 2005 date).*
>
> c. there is an "adsoft" transaction dated January 4th, 2006 and posted January 6th, 2006 in the amount of $95.28 (79.99 US dollars).

Search Warrant

[38] On August 28, 2007, Sgt. Johnson attended before Judge John Faulkner and obtained a search warrant for the residence of Mr. Cafferata, the vehicle licensed KNOBAH, plus any outdoor facilities at Mr. Cafferata's residence. In the ITO, Sgt. Johnson reiterated essentially identical information to that contained in the Affidavit, as supplemented by the NorthwesTel IP address information and the CIBC banking documents.

[39] There was also some additional information in the ITO from Sgt. Johnson's two conversations on August 23 and 28, 2007 with Dr. Matt Logan, an Operational Psychologist in the RCMP Behavioural Sciences Unit, to gain insight into the behaviour of people who have Paraphalia and fantasies fed by pornography. Given that there are certain assumptions underlying Dr. Logan's opinions, which I am not prepared to make with respect to their application to Mr. Cafferata, I consider the information in paragraph 24 of the ITO to be of no probative value for the purposes of my decision.

[40] Further, the ITO states that on August 28, 2007, RCMP Cst. Natasha Dunmall attended 45 Cottage Lots in Teslin and noted signs of occupation and a vehicle with the license plate "KNOBAH" parked in the driveway.

Law and Analysis:

Production Order/Search Warrant

Statutory Authority

[41] Section 487.012 of the *Criminal Code* authorizes a justice or judge to make a production order for documents or data where the justice or judge is satisfied that there are reasonable grounds to believe that:

(a) an offence against this Act or any other Act of Parliament has been or is suspected to have been committed;
(b) the documents or data will afford evidence respecting the commission of the offence; and
(c) the person who is subject to the order has possession or control of the documents or data.

[42] Section 487(1) authorizes a justice to issue a search warrant where the justice has reasonable grounds to believe that there is in a building, receptacle or place:

(a) anything on or in respect of which any offence against this Act or any other Act of Parliament has been or is suspected to have been committed;
(b) anything that there are reasonable grounds to believe will afford evidence with respect to the commission of an offence, or which will reveal the whereabouts of a person who is believed to have committed an offence, against this Act or any other Act of Parliament;
(c) anything that there reasonable grounds to believe is intended to be used for the purpose of committing any offence against the person for which a person may be arrested without warrant; or (c.1) any offence-related property.

[43] The standard constituting "reasonable grounds to believe" is summarized in ***R.*** v. ***Sanchez***, (1994), 93 C.C.C. (3d) 357 (Ont. Gen. Div.) at paras. 28-29 as being one of "credibly-based probability".

> 29. Mere suspicion, conjecture, hypothesis or "fishing expeditions" fall short of the minimally acceptable standard from both a common law and constitutional perspective. On the other hand, in addressing the requisite degree of certitude, it must be recognized that reasonable grounds is not to be equated with proof beyond a reasonable doubt or a prima facie case. The appropriate standard of reasonable or credibly-based probability envisions a practical, non-technical and common sense probability as to the existence of the facts and inferences asserted (citations omitted).

[44] In ***R.*** v. ***Morris***, (1998) 134 C.C.C. (3d) 539 (N.S.C.A.) at para. 30, Cromwell J.A. stated:

> (i) The information to obtain the warrant must set out sworn evidence sufficient to establish reasonable grounds for believing that an offence has been committed, that the things to be searched for will afford evidence and that the things in question will be found at a specified place

(ii) The information to obtain as a whole must be considered and peace officers who generally prepare these documents without legal assistance, should not be held to the specificity and legal precision expected of pleadings at the trial stage
(iii) The affiant's reasonable belief does not have to be based on personal knowledge, but the information to obtain must, in the totality of the circumstances, disclose a substantial basis for the existence of the affiant's belief
(iv) Where the affiant relies on information obtained from a police informer, the reliability of the information must be apparent and is to be assessed in light of the totality of the circumstances… (citations omitted).

[45] The Affidavit or ITO used to obtain a Production Order or Search Warrant requires the following:

1. There is a legal obligation for full and frank disclosure of material facts. It need not be lengthy or detailed, and does not need to include every minute detail of the police investigation
2. It must set out the facts fully and frankly
3. It should never attempt to trick its readers (See ***R.*** v. ***Araujo***, 2000 S.C.C. 65 at paras. 46-47)

Standard of Review

[46] In assessing the validity of the Production Order and the Search Warrant, the presumption is that they are valid. Therefore Mr. Cafferata bears the burden of demonstrating that they are invalid***.*** (See ***Quebec (Attorney General)*** v. ***Laroche***, 2002 S.C.C. 72 at para. 68.

[47] The standard for reviewing the sufficiency of the information before the justice or judge who issued the search warrant is to determine whether there was sufficient sworn information before the justice or judge that he or she could have issued the warrant; not whether the issuing judge should have issued the search warrant. The reviewing judge is not to second guess the issuing justice or judge, or substitute his or her decision, but determine whether there was any basis upon which the authorizing justice or judge could be satisfied that the relevant statutory preconditions in ss. 487(1) and 487.012(3) existed.

> The test is whether there was reliable evidence that might reasonably be believed on the basis of which the authorization could have issued, not whether, in the opinion of the reviewing judge, the application should have been granted at all by the authorizing judge. (See ***R.*** v. ***Al-Maliki***, 2005 BCCA 157 at para. 19)

[48] The reviewing judge can also consider additional evidence that was not available to the issuing judge, thus amplifying the information. This additional information can either support or undermine the grounds for obtaining the production order and/or search warrant. The use to which any such additional evidence is to be put is to determine whether there continues to be any basis for the decision of the authorizing judge (See ***R.*** v. ***Morelli***, 2008 SKCA 62 at para.19; ***R.*** v. ***Brown***, 2007 B.C.P.C. 448 at paras. 117-119)

Errors

[49] Errors in the information that has been provided to the issuing justice or judge do not automatically invalidate the search warrant. Any incorrect information must be excised and the remainder of the evidence considered as amplified by any evidence given on the *voir dire.* (See ***Morelli*** at paras. 20, 21)

Hearsay

[50] It is not uncommon, in fact it is almost invariably the case, that the Affidavits and ITOs utilized to obtain Production Orders and Search Warrants are based on hearsay, and sometimes even double or triple hearsay statements. The use of hearsay evidence is not improper so as to adversely effect the validity of an authorization or warrant subsequently issued, although there remains an issue as to assessing the reliability of the statements (See ***Brown*** at paras. 68-69).

[51] A mere statement of criminal activity relayed by a party, even if the party is considered to be reliable, to an informant is insufficient unless enough of the underlying circumstances that give rise to the conclusion reached are disclosed.

If the hearsay is obvious on the face of the Affidavit or ITO it cannot, however, be said to have misled the issuing judge. (See ***Brown*** at paras. 73, 85-90)

Boilerplate

[52] Boilerplate language can have the minimal effect of wasting paper and the reader's time, or it can "…trick the reader into thinking that the affidavit means something that it does not". The important consideration when assessing a police officer's use of apparently boilerplate language is to "…determine if the officer automatically followed boilerplate wording without any comprehension or whether the words actually reflected informed knowledge". It is important to look behind the actual words used, to consider whether the officer took steps to adequately inform him or her self of what the meaning was of what he or she was saying. When the use of such language forms part of the narrative investigation of facts, it may not detract from the sufficiency of the factual information in the Affidavit or the ITO. (See ***Brown*** paras. 100, 105-108)

Conclusory statements

[53] Conclusory statements without evidence in support of these statements are generally to be avoided because they "give the authorizing justice no independent basis for making an assessment". That said, "some deference should be paid to the ability of a trained peace officer to draw inferences and make deductions which might well elude an untrained person…Probable cause does not arise, however, from purely conclusory narrative". In considering whether a statement is conclusory, the statement must be considered in light of the totality of the evidence in the Affidavit or ITO. If, after such a consideration, a statement is misleading, it should be excised from the Affidavit or ITO. (See ***Sanchez*** at para. 20; ***Morelli*** at para. 24; ***Brown*** at para. 104)

Arguments of Counsel

Summary

[54] In its simplest form, the argument by counsel for Mr. Cafferata is that both the Affidavit for the Production Order and the ITO for the Search Warrant contain conclusory statements, boilerplate information, are full of assumptions, contain incorrect information, and are at times misleading. As such, after either excising or otherwise assessing the appropriate weight to be given to these problematic aspects of the Affidavit and ITO, both the Affidavit and the ITO fall below the threshold test for admissibility as being suspicion only and do not give rise to the required credibly-based probability. Defense counsel maintains this position while conceding that the privacy interest in the bank records is less than that for the residence, outbuildings, and vehicle of Mr. Cafferata.

[55] Counsel further argues that there was insufficient investigation by the Whitehorse RCMP into the underlying details of the initial investigation by the Department of Homeland Security that resulted in the information about Mr. Cafferata being sent to the NCECC, and then to the RCMP in Whitehorse.

[56] Counsel says that there was insufficient information about “Adsoft” to conclude that this entity was involved in, or purported to be involved in, exclusively, the sale and distribution of child pornography. Sgt. Johnson testified that he had little information about Adsoft other than it was used as a “front” or “ruse”, and he agreed that the Affidavit and ITO are conclusory in relation to Adsoft being a child pornography distributor. He stated that he was informed by Sgt. Payne that the Department of Homeland Security would not disclose more information about Adsoft. He was not provided any explanation as to why they would not do so. Sgt. Johnson did not do any independent search on Adsoft until just recently.

United States of America v. ***Payne*** (U.S. District Court New Jersey) Docket #07-226)

[57] Mr. Parkkari puts forward the case of ***USA*** v. ***Payne*** as a template, more or less, of what type of investigation should be undertaken, and information obtained as a result, in order to justify the issuance of a warrant. I will refer to this case at some length due to its similarities with the factual background in the case at bar.

[58] As Mr. Parkkari points out, the ***Payne*** case appears to be connected to the same investigation that resulted in the information concerning Mr. Cafferata's alleged participation in accessing child pornography being ultimately forwarded to the RCMP in Whitehorse. That said, I want to make it clear that I have not relied on any factual aspects of the ***Payne*** case in assessing the applicable facts in the case before me.

[59] The affidavit in support of the application for the search warrant in ***Payne*** was broken down into three sections:

1. background information concerning computers and the internet, including how such technologies have affected the nature of child pornography trafficking and possession;

   - The affiant had been a United States Immigration and Customs Enforcement (ICE) agent for almost 5 years and had participated in executing more than 40 search warrants for similar child pornography investigations. Her evidence provided an outline of the internet's effect on the methodology of the production, dissemination, accessing and storage of child pornography.

2. the nature of the ICE "New Jersey Investigation" of a commercial website labeling itself Illegal.CP, which offered access to thousands of images and videos of child pornography via a subscription service;

   - the commercial website Illegal.CP offered access to child pornography through a subscription service. Its three components consisted of 1) a banner page that urged the viewer to "Join Now". This banner page was located at a URL site and contained several images of child pornography. It served as an advertisement and gateway to the subscriptions-only portions of the Illegal.CP website. If "Join Now" was clicked, an application page appeared requesting personal and credit

card information in order to create a subscription; 2) a login page where subscribers could enter the login and password to gain access to the contents of Illegal.CP; and 3) the Illegal.CP website itself with images and videos of child pornography.

- An undercover agent purchased access to the Illegal.CP site, entered personal information, received an e-mail from what was called the "Dykstra Account" with a login and password and a notification that $79.99 would be charged to his credit card under the name ADSOFT. The agent then used the login and password and accessed a child pornography site with thousands of images. The initial page on the site had a Frequently Asked Questions section and warned of the illegal nature of the site and how to avoid liability.
- The ICE agents located the server, obtained a search warrant and, besides locating child pornography, found IP addresses for all contacts with the server for specified time periods.
- A wiretap was then authorized for the Dykstra Account for several periods of time, including the time frame for the case at bar. These intercepts allowed the ICE agents to determine how subscriptions to Illegal.CP were processed and approved, including that the subscriber's personal information was sent to the Dykstra Account, and then transmitted to a third account which verified the information, and approved or denied the application in an e-mail back to the Dykstra Account. If approved, the Dykstra account would then send an e-mail to the subscriber providing the login, password and access to the Illegal.CP site, as well as notification of the charge incurred.
- The contents of the Illegal.CP site were transferred to a new server. A search warrant issued in respect of this new server provided additional subscriber information such as identification, login, e-mail address, IP address and the date and time that the subscription began.

3. the evidence establishing the Defendant, Payne, subscribed to the Illegal.CP website.

    - ICE agents intercepted an e-mail from the Dykstra Account to a third e-mail account joe777@mail.ru, which was responsible for verifying the information and approving or denying a subscription application. This e-mail contained Mr. Payne's name, home address, e-mail address, credit card number with three digit code, selected login, password and IP address. *I note in these written reasons that during my oral rendering of judgment I mistakenly stated that this e-mail went to Mr. Payne's e-mail address* (I also note that this e-mail intercept would appear to correspond to the Canadian Subscribers.xls data spreadsheet in paragraph 11(a) in the Affidavit and ITO in the in the case at bar*).* The next day, another intercept of an e-mail to the Dykstra Account from a third account confirmed the approval of Mr. Payne. (I note that this would appear to correspond to what is

contained in paragraph 11(b) of the Affidavit and ITO in the Canadian Adsoft Transactions.xls data spreadsheet in the case at bar). That same day, an e-mail from the Dykstra Account to Mr. Payne was intercepted. This e-mail included confirmation of a 20 day membership in the site, notice of $79.99 billing by Adsoft, the same login and password and three links to the Illegal.CP site. (I note that there is no evidence in the case at bar that Mr. Cafferata actually received a login, password and links to a child pornography website).

- Due to limited availability of access to the log files for the Illegal.CP servers, ICE agents were unable to confirm that Mr. Payne ever accessed images from the Illegal.CP website after being granted access.
- ICE agents then took steps confirming that the IP address belonged to Mr. Payne, and was associated with the same home address and telephone number.
- The ICE agents also subpoenaed the credit card records for Mr. Payne and determined that his credit card number connected to the Dykstra Account e-mails had been charged $79.99 by Adsoft.
- As a final step, the ICE agents confirmed through third party records and surveillance that Mr. Payne lived at the address linked to the Dykstra e-mails.

[60] Based upon all the above information, ICE agents obtained a warrant to search Mr. Payne's apartment for child pornography.

[61] Defense counsel for Mr. Payne argued that the search was a violation of Mr. Payne's rights, in part, as there was a lack of probable cause to obtain the warrant.

[62] The legal test in the United States is similar to that in Canada, in that it requires, from a practical or common-sense point of view, that there must be a fair probability that contraband or evidence of a crime will be found in a particular place. The issuing magistrate's decision is given considerable deference by the reviewing court which is required to "simply ensure that the magistrate had a substantial basis for concluding that probable cause existed".

[63] The court in ***Payne*** dismissed defense counsel's application because the affidavit:

- outlined the investigation in detail
- explained at length the ICE's familiarity with the method of subscribing to Illegal.CP
- described the transmission of Mr. Payne's personal and financial information to the Dykstra Account which had been verified by the agents as being the means of initiating a subscription to Illegal.CP
- outlined the ICE agents thorough independent investigation linking the personal and financial details in the Dykstra Account e-mails to Mr. Payne and his home address
- most telling of all, established that Mr. Payne used his credit card to pay $79.99 for a subscription and that he did not subsequently challenge the charge to his credit card.

[64] The court found that all of this information taken in combination clearly supported a reasonable inference that Mr. Payne subscribed to Illegal.CP. The court further concluded that it neither strained logic nor defied common sense to conclude that an individual who pays $79.99 for a subscription to a child pornography website has done so because he intends to view and download its content. The court then stated that the reasonable inference was that Mr. Payne would have used his subscription to access Illegal.CP and download images and that these images would be found in his home.

[65] The court expressly rejected the defense argument that the lack of evidence pointing to Mr. Payne ever actually accessing Illegal.CP, or downloading images of child pornography, undermined probable cause as a basis for the issuance of the warrant.

[66] The court also rejected the argument of defense counsel that evidence of a subscription alone cannot support probable cause. The court stated that the affidavit provided ample circumstantial evidence particular to Mr. Payne to support a reasonable inference being drawn about child pornography being found in his home.

[67] There were also no allegations that the group Mr. Payne sought to join ostensibly conducted legal activities; in fact it boasted to possessing the best child pornography on the internet. The warning upon joining the site was that its contents were considered illegal in all countries and subscribers were advised of a method of evading punishment if caught. The Illegal.CP site required payment and subscribers had to take several steps to join.

[68] The court also rejected other defence counsel arguments, including one that the various URLs did not contain any overt references to child pornography, on the basis that the ICE agents' documentation of established patterns allowed for a common sense acceptance that there was a fair probability that the $79.99 payment to Adsoft was for a paid subscription to a child pornography site, rather than for some innocent, mistaken or wholly unrelated purpose. The affidavit stated that the e-mail from the Dykstra Account to Mr. Payne provided three URL links to the Illegal.CP website.

[69] Counsel for Mr. Cafferata points to the following deficiencies in the Affidavit for the Production Order and in the Information to Obtain:

1. the advertising banner has no links to Mr. Cafferata;
2. the investigation could not determine what sign-in page Mr. Cafferata was on;
3. the intercept only captures personal credit card information provided by Mr. Cafferata to the e-mail account accessed from the "Join Now" page. There is no return e-mail ever received by Mr. Cafferata or processed, no confirmation that Mr. Cafferata was approved as a subscriber, there are no logins and passwords provided to Mr. Cafferata, and no log files showing anything was ever accessed at a child pornography site by Mr. Cafferata.

[70] Defence counsel also challenges the sufficiency of the Affidavit and the ITO on other points.

1. the background information in paragraphs 7 and 8 of both is third and fourth hand from the US or other agencies, albeit recognizing that it is provided by law enforcement agencies rather than a confidential informant, and thus has more credibility. *(Although not stated in my oral judgment, my notes during submissions on the voir dire referred to paragraphs 7 and 8; It may in fact have been paragraphs 8 and 9 that Mr. Parkkari was referring to).*
2. paragraph 8(b) only mentions one intercept for the period from December 27, 2005 to February 25, 2006, while there were in fact at least two, as well as one or more warrants. This leaves the impression that any information captured came from the one intercept, including the information contained in paragraphs 11(a) and 11(b).
3. paragraph 8(c): Sgt. Johnson did not know exactly what was intercepted or which of the two intercepts in this 60 day period pertained to which e-mails. Sgt. Johnson did not have first hand information regarding this, and what information he had came from Sgt. Payne. Sgt. Johnson cannot say whether this is "boilerplate". For example, of 83 subjects, 19 of them had records caught of sites they visited containing child pornography, 12 had application information captured with the corresponding Adsoft transaction, (defense counsel submits this was probably by warrant rather than by intercept), and 53 individuals had just the subscription information captured. Does the "each" refer to all 83 individuals? It is not clear. Paragraph 8(c) does not point out that there was no customer service number provided for Mr. Cafferata. The bottom line argument is that the same paragraph captures everyone without distinction, thus being somewhat "boilerplate" in the lack of discrimination between the 83 identified individuals.
4. paragraph 8(d) may have had some editing, but Sgt. Johnson could not provide information as to whether all the content was provided or whether there was some editing. There is no information as to whether adult pornography was also available for access. It is a conclusory statement without background. It doesn't say how many images, the nature of these images, or whether any or all of them were legal or illegal.
5. paragraph 8(e) utilizes the word "some" which is unclear. What is the rest of it outside of "some"? Again, do any of the pornographic websites contain legal images that subscribers can access? There is an insufficiency of information provided and a lack of forthright or full disclosure from the US authorities. There are conclusions but no background for these conclusions. For example, in paragraph 9(g) Adsoft is called a "company" but what is meant by "company" – is it a legally registered company? There is insufficient information.
6. paragraph 9(b) - 35 URLs, out of a larger number, were captured for all the Canadian targets, but not every one of the Canadian targets and not all the URL's contained the named banners. Without more specific detail, this paragraph is misleading. The Affidavit and the ITO do not make it

clear that there was no evidence that Mr. Cafferata ever utilized one of the URLs

7. paragraph 9(c) is conclusory. For example, there is no such intercept for an e-mail to Mr. Cafferata, so how can it be said that "he would have". This paragraph leaves the assumption that everyone who subscribed would have received the e-mail and viewed the pop-up. This assumption is not realistic and probable. Just as a credit card can be proffered at a store, offering it up is not evidence it was actually approved for use and a purchase made. The general information as to process misled the issuing justice and judge, as the Affidavit and ITO are fairly silent on the absence of links to Mr. Cafferata. Sgt. Johnson's testimony could not assist with anything more than speculation as to why an e-mail to Mr. Cafferata was not intercepted.

As I understand this argument by defence counsel, his submission is that there is a danger that it could be inferred that these steps were completed in the case of Mr. Cafferata, when in fact there is less evidence of a connection to him in this case to the process than was evident in the ***Payne*** case. While the generalities as to process may be fine, there is a lack of clarity as to what constitutes the evidence connecting Mr. Cafferata to the process, thus creating a misleading effect from the use of this "conclusory" or "boilerplate" investigation information.

8. paragraph 9(f): There is no clear message date, as this date was calculated after-the-fact, and no sysdata date for Mr. Cafferata. There is no factual background to explain this statement and therefore we are left with a conclusory statement. There is no "presumption" in operation here. Sgt. Johnson should have asked for background information to support the conclusory statements. How do you come up with a message date if there is no sysdata date? There should have been follow up steps in order to obtain an explanation. Is it enough to say "here is what they are telling me" without enquiring or determining "why they are telling me this"?
9. paragraph 9(g): The phrase "would show", is a conclusory statement in respect of Mr. Cafferata. It may not have been problematic if clearly confined to being a narrative of the process. It does not, however, say for example, "would show if transaction approved". (although I note that this may be a common sense presumption the reader would reasonably be expected to apply). The statement that Adsoft is a "front company for the criminal organization administering access to these child pornography websites" is conclusory without evidentiary foundation. Sgt. Johnson testified that he understood that "Adsoft purported to sell something but it didn't", and that this was information that he had at the time of preparing

the ITO. He agreed that he had no factual background to support this statement. He was simply told this by Sgt. Payne. This results in what Mr. Parkkari terms a "bait and switch", in that maybe something legal gets routed to the same Adsoft. The US investigative authorities do not provide information as to whether Adsoft is related to anything other than child pornography.

10. paragraph 9(h) is misleading in that none of the referer sites listed were captured for Mr. Cafferata. The wording at the bottom that "*not all the referrer sites were captured for every suspect which was the case with Cafferata" leads to the inference that at least one of these sites was captured for Mr. Cafferata, but not all of them.
11. paragraph 10(c) is conclusory as Sgt. Johnson testified he was told this by "maybe" Daniel Lacroix, but he cannot say whether Daniel Lacroix did the work to determine this. Sgt. Johnson should have asked himself why he could say that. Defense counsel submits, admittedly, that this is just one small part of the whole.
12. paragraph 11: The phrase "would have been captured" is conclusory. Paragraph 11(a) shows information being provided by Mr. Cafferata. It is a request for a transaction. Paragraph 11(b) shows information sent to Mr. Cafferata, (again, as I understand it, to an intermediary account with the next step, not evidenced in this case, of an e-mail from this intermediary account to Mr. Cafferata). As stated earlier, paragraph 11(b) was a response to a different request in April 2006. While paragraph 11(b) clearly should be excised from the Affidavit, defense counsel submits that it should also be excised from consideration as amplified evidence in assessing whether the Search Warrant could have been issued, as we don't know where it came from. He submits that we don't know its reliability other than being from the US investigation. We don't even know the date of the intercepts.

    Defence counsel submits that while, in the continuum, the Crown is on its way to an attempt to access child pornography, the evidence falls short of actually linking Mr. Cafferata to having accessed child pornography. We do not have the information in paragraph 11(b) which would progress the Crown further down the continuum, albeit not far enough. The authorizing justice and judge did not know this. All that remains in the end regarding Mr. Cafferata, is that information was sent to an e-mail address that purported to sell something else but did not. Was there another page that dealt with an application for the "purported sale"?

13. paragraph 13: There was no direct evidence that Mr. Cafferata was ever granted access or that he was a subscriber to a child pornography site. This was not made clear in the Affidavit or the ITO. The wording in this paragraph could leave the impression that Mr. Cafferata was in fact a confirmed subscriber. It says what Mr. Cafferata "would have seen" if they had been able to establish that he in fact ever gained access. Sgt.

Johnson could not explain why certain things were “blank”. He agreed that information would likely have to be accurate in order for the credit card transaction to be approved, (which I note, however, is also expressly stated in paragraph 11 of the Affidavit and ITO). He also agreed that it may have been possible for an applicant to be rejected, and that there would not necessarily be a return e-mail stating this to be the case. Sgt. Johnson further agreed that there was no confirmatory e-mail to Mr. Cafferata indicating that he was approved as a subscriber.

14. paragraph 18 is similar to the position of Richards J. in the ***Morelli*** dissent; you cannot “bootstrap” an argument to find that the existence of an application leads to the existence of a download by Mr. Cafferata, an existence which has not been established on the evidence. As there was no evidence of a download it cannot be assumed that there is therefore anything on the computer to keep and thus no reasonable grounds to believe a search for the items listed in the Search Warrant, in the specified locations would provided evidence of accessing or possessing child pornography.
15. paragraphs 19-21 of the ITO should be excised as only resulting from the Production Order which should have not been granted. If, however, the Production Order is upheld and these paragraphs are not excised from the ITO, then what is left is an application by Mr. Cafferata to access a child pornography website and a Visa transaction matching the application. While the Crown would be further along the continuum, it remains deficient as there is no confirmation of a download of child pornography. Maybe the recipient of the $79.99 from Mr. Cafferata took the money and ran. As he says, who would go to bank and challenge the charge on the basis of not receiving what was paid for, if the purchase was child pornography?
16. paragraph 22 of the ITO should be excised as it refers to the credit card documents resulting from the issuance of the Production Order, which should be declared invalid. Even if the Production Order is not struck down and paragraphs 19-21 of the ITO stand, paragraph 22 should be excised as the “adsoft” transaction data referred to is from paragraph 11(b), which is itself insufficiently reliable.

<u>Crown submissions</u>

[71] Crown counsel submits that it is important to look at the big picture and keep in mind that Mr. Cafferata is charged with accessing child pornography as well as possessing it. In seeking the Production Order, Sgt. Johnson was looking for information to corroborate the existence of an internet transaction providing Mr. Cafferata access to a child pornography site. This was a corollary

investigation to confirm suspicion of the type of transaction that they expected to find.

[72] Crown counsel concedes that one problem is the lack of return information to Mr. Cafferata confirming that his application had been approved.

[73] He also concedes that the evidence Sgt. Johnson thought that he had at the time he obtained the Production Order and the Search Warrant has changed materially.

[74] Crown counsel agreed that paragraph 11(a) of the Affidavit and ITO had the potential to mislead the authorizing justice or judge in that the meaning of "http_referer: (nothing)" was not explained within the Affidavit or ITO.

[75] The Crown agrees that paragraph 11(b) must be either excised or have the weight attributed to it attenuated considerably, as must all references to Adsoft that flow from paragraph 11(b). This material change gives rise to some reasonable concerns about the evidence being strong enough to get beyond accessing to possession and then to the actual downloading of child pornography by Mr. Cafferata.

[76] He points out, however that this error was nothing more than an innocent mistake, and not in bad faith or with any deliberate attempt to mislead.

[77] Crown counsel agrees that everything in paragraph 9(g) regarding Adsoft being a front company for criminal activity should be disregarded as it is completely unsourced. He points out, however, that there is no evidence that Adsoft does anything else and that properly sourced background information as to how the process works does place Adsoft within the process.

[78] He states that the Production Order was a critical necessary intermediate step to get to the existence of a justifiable basis for the issuance of the Search Warrant.

[79] In sum, Crown counsel argues that an analysis of the logical and reasonable information by someone in the shoes of an ordinary reasonable person would cause this person to conclude that the system works as detailed, and that someone at Mr. Cafferata's computer address applied for access to a child pornography website, and provided personal information for a $79.99 USD transaction. This person would draw the inference that this transaction was carried out, and that evidence of this transaction would be available on Mr. Cafferata's credit card information and on his computer. It is allowable to draw reasonable inferences from the information provided and available, and the question is whether a reasonable person acting judiciously could issue the order. There is, says the Crown, a compelling case that Mr. Cafferata, or someone pretending to be him, tried to access child pornography through the internet by the use of a credit card. The reasonable inference to be drawn is that the $79.99 is for the same product, even if other things were available. This is not to say that there is any such evidence of other products that could be purchased.

[80] Crown counsel submits that the balance of the RCMP investigation was to take every reasonable step possible to confirm it was Mr. Cafferata. He points to Mr. Cafferata's distinctive license plate "KNOBAH", corresponding to the login in the spreadsheet in paragraph 11(a) of the Affidavit and ITO, and an apparent problem with a different telephone number that was ultimately, through investigation, linked to Mr. Cafferata's work rather than his home.

[81] Crown counsel submits that this was clearly an apparent attempt by Mr. Cafferata to access child pornography. The logical steps for the RCMP to take upon learning of this apparent attempt were to see if there was there a transaction, hence the Production Order, to then see if there was actual access

and whether such access was evidenced on the computer, hence the rationale for seeking the Search Warrant (and for the authorizing judge to find that he had grounds to issue it.)

Findings and Conclusion

[82] Other than the Adsoft being a “front for criminal activity” reference, and some potential for the authorizing justice and judge to have been misled or to have drawn erroneous inferences, which I will discuss below, I do not share the same concerns as defence counsel about the use of conclusory statements and boilerplate language in the Affidavit and the ITO. Most of these statements, although originating from sources other than Sgt. Johnson, provide a foundational investigative narrative for the information provided to Sgt. Johnson. They were filtered through experienced personnel within the NCECC, who met with the US investigative authorities, rather than coming directly and unfiltered to Sgt. Johnson.

[83] Although he had some limited experience in the area of internet child pornography, Sgt. Johnson took considerable steps to follow up with both NCECC officers and Sgt. Riccitelli in order to confirm and understand the meaning and relevance of the documents that were provided to him. It is clear that he was frustrated at times with his inability to obtain all the information he was requesting. There is no doubt that there was non-disclosure of certain investigative details by the US authorities, but they may well have had their own legitimate reasons not to disclose more information to Sgt. Johnson. This non-disclosure impacts to some extent on the reliability of the information provided as to the process and Mr. Cafferata’s actions within it, but to a large extent, other than aspects I will deal with further on, this impact is offset by the fact that Sgt. Johnson was relying on information provided by specialized professionals within the law-enforcement field.

[84] I am not concerned about the fact that there were two intercepts, rather than one, for the period from December 27, 2005 to February 25, 2006. Sgt. Johnson testified that he saw this as being, in effect, one intercept. Although he was technically incorrect, there was nothing misleading in this technical error that could have had any substantive effect on the decision of the authorizing justice and judge.

[85] I also do not share defence counsel's concern about the possibility that the subscription page could have allowed for the purchase of items other than child pornography, that it could have been accessed by accident, or that Sgt. Johnson could not provide more details one way or the other on these points. This, in my mind, on the evidence before me, is primarily speculation as to the existence of other possibilities that are not apparent on the face of the evidence in the Affidavit, the ITO or the testimony of Sgt. Johnson.

[86] This latter argument is somewhat similar to those made by counsel for the applicant in ***R.*** v. ***Ward***, 2008 ONCJ 355. In ***Ward***, defence counsel argued that the authorizing judge may have arrived at a different conclusion had he possessed additional technological information, including technological information pointing to the possibility of the accidental accessing of child pornography. The following points were listed by the court in para. 79:

> **79.** In terms of information not provided or insufficiently provided, the applicant points out the following:
> • That there is not evidence he knowingly accessed child pornography;
> • That there is little or no evidence provided about technological information explaining how images or information was or could be accessed;
> • That there is not evidence about his on-line activities relevant to the issue of whether he was viewing pornography material knowingly and intentionally;
> • That little or no information was provided about the appearance of the website pages;
> • That there is a lack of description of the forums available on the website;
> • That information provided, namely names "Los Corsa Rios" and "Naturally boy s2027" are insufficient to suggest a user would recognize the content as being child pornography;

> • That the images shown are insufficient to suggest the male subjects were children and not adults;
> • That only a small number of forums contained child pornography in comparison to all other forums available.

[87] In ***Ward***, expert evidence was called by defense counsel to provide this additional technological information. The court rejected this argument, pointing to its speculative nature, and suggesting that some of the issues raised would be better left for a defence at trial. The court stated the following in para. 96:

> …It was not necessary for [the issuing judge] to decide whether the available information afforded sufficient evidence to result in a conviction. The police compiled a satisfactory summary of events. Nuances, matters of interpretation, alternative possibilities, issues involving the weighing of evidence and matters concerning the existence of other possible inferences need not all be factored in at the application for the search warrant stage.

[88] The court in ***Ward*** found that the basis core information was enough to have justified the issuance of the warrant.

[89] Although there is, as pointed out by Mr. Parkkari, some ambiguity in the Affidavit and the ITO as to whether all of the images that could be accessed by an approved subscriber were child pornography or were intermingled with other images, there is the evidence of Sgt. Johnson during the *voir dire* that all the images were child pornography. The foundation for his statement was not deeply probed or evidenced, but in my mind this is not particularly significant. For the purposes of obtaining the Production Order and the Search Warrant, I would be satisfied that even if the evidence showed intermingling, and I find that the evidence here does not specifically show that there was any intermingling, that this would still provide a sufficient basis for the issuance of the Production Order and the Search Warrant, in order to allow for further investigation. It would be illogical to allow individuals to potentially escape criminal liability for accessing or possessing child pornography on the basis that not all the images accessed or possessed were illegal.

[90] I do share defence counsel's concerns about the following deficiencies in the Affidavit and the ITO, many of which are not so much what was stated, but what was not stated, and the potential for these omissions to have misled the authorizing justice and judge:

1. they did not point out that there was no customer service number provided for Mr. Cafferata;
2. they did not make it clear that none of the 35 URLs connected to Canadian subscribers were associated with Mr. Cafferata;
3. they did not state that there was no return e-mail provided to Mr. Cafferata in response to his making the application to be approved as a subscriber;
4. they did not state that none of the 14 captured referer sites were captured for Mr. Cafferata, and therefore could be read as suggesting otherwise by the poor wording used;
5. paragraph 11(b) related to a different intercept and transaction than what it was believed to be associated with, and what was put forward to the authorizing justice and judge.
6. they do not make it clear that there was no evidence that Mr. Cafferata was granted access to or in fact did access a child pornography site. In fact, the wording about the process (to some extent boilerplate and conclusory), had the potential to leave the impression that Mr. Cafferata was a subscriber, and that he did access such a site.

[91] To a lesser extent, I have some concerns about the lack of a "sysdata date" and time on the Canadian Subscribers.xls spreadsheet, in the absence of an explanation for this absence. I am not, however, particularly concerned about the message number date. I find that the information provided to Sgt. Johnson by Sgt. Riccitelli is sufficient even without further explanation as to how the US investigators actually determined this date after the fact. On the whole of the information, and considering the relatively lesser significance of the message number in the larger scheme, I am prepared to accept their professional expertise in this instance as to how the US investigators arrived at the date.

[92] With respect to the potential to mislead the authorizing Justice or Judge through these omissions and errors, I am not going to presume in this context that they did in fact do so. While potentially misleading, the wording in the

context of the totality of the evidence in the Affidavit and the ITO could, for the most part, also have simply been viewed for what it was, an explanation as to the general process. There are no statements regarding Mr. Cafferata that have any apparent intent to mislead on their face, or clear wording indicating a factual connection between Mr. Cafferata and a particular part of the process, that there was not direct evidence of. Even paragraph 11(b) was not put forth with strong or clear wording to the effect that this was a return e-mail confirming that Mr. Cafferata had been approved as a subscriber, or that he was actually provided a login and password for access to a child pornography site.

[93] In the end, what I am left with is a fairly detailed explanation as to the general process that culminates in any particular individual accessing child pornography websites. I am left with a somewhat less detailed explanation of the process of intercepting the information pertaining to these subscribers. This includes the hit-and-miss nature of the investigation with respect to access to http_referer sites, e-mail correspondence going either direction, and actual access to child pornography websites.

Production Order

[94] With respect to the issuance of the Production Order for Mr. Cafferata's bank records, I find that the evidence, after I excise from the Affidavit paragraph 11(b), is that Mr. Cafferata applied for a subscription to a child pornography website. I also am satisfied that I have reasonable and reliable evidence of the general process. While there is no direct evidence that Mr. Cafferata did not obtain access to a child pornography site, there is also no evidence that he did, even though there appeared to be a sporadic intercept capacity within the US investigation capable of confirming this. In this context, is this attempt to access child pornography a sufficient basis such that the justice could have issued the Production Order?

[95] Section 487.012 requires that the authorizing justice be satisfied that there are reasonable grounds to believe that certain documents or data will be found at a specified location and that these documents or data will afford evidence respecting the commission of an offence or suspected offence. I am satisfied that Cst. Bechtel had reasonable grounds to believe that the banking documents at the CIBC pertaining to the Visa account in Mr. Cafferata's name that was provided in the subscription application, would afford evidence, at a minimum, of the offence or suspected offence of accessing child pornography. I refer to the case of ***R.*** v. ***Missions***, 2005 NSCA 82, cited in para. 68 of ***Morelli***, where Roscoe J.A. stated at para. 21:

> …The normal inference that one intends the natural consequences of one's actions is applicable to computer usage just as it is to any other human activity, especially in light of the lack of evidence to rebut the inference.

[96] It was reasonable for Sgt. Johnson and Cst. Bechtel, based upon the information provided to him by Sgt. Johnson, to draw the inference that if Mr. Cafferata applied to be granted access to a child pornography website and provided his credit card number for payment in connection with the application, he may well have been granted access to the website. He would then have used his right of access to commit the offence of accessing child pornography. There were therefore reasonable grounds to believe that confirmation of a Visa transaction in the relevant time period for $79.99 USD would be found in the Visa documents in possession of the CIBC. This was a prudent investigative step, and had a significantly lesser interference with the privacy rights of Mr. Cafferata than seeking to obtain a search warrant for his residence and computer would have been at that stage.

[97] In reaching my decision I have weighed the impact of the failure of the Affidavit to clearly articulate what was not captured through the intercepts in respect of Mr. Cafferata. I find that these failures, in circumstances where the evidence points towards an overall pattern of sporadic captures, and even

without Sgt. Johnson being able to explain with any certainty why these gaps exist, do not undermine the basic fact of an apparent attempt by Mr. Cafferata to access child pornography.

[98] As such, I am satisfied on the evidence that the authorizing justice had the requisite reasonable grounds such that he could have issued the Production Order.

Search Warrant

[99] The application for the Search Warrant adds to the evidence in the Affidavit by including the confirmation of the $79.99 transaction to Adsoft from the credit card records of Mr. Cafferata, with a transaction date of January 4, 2006 and posted on January 6, 2006.

[100] Section 487(1) of the *Criminal Code* requires that the authorizing justice or judge be satisfied that there are reasonable grounds to believe that there will be found at a specified location anything that there are reasonable grounds to believe will afford evidence respecting the commission of an offence or suspected offence.

[101] The fact that Mr. Cafferata applied for a subscription to a child pornography website and apparently had the subscription amount of $79.99 charged to his credit card account, is not proof that he actually was granted access to a child pornography website or that he, if granted access, ever actually viewed images on a child pornography website. I find, however, that this evidence provided Sgt. Johnson with reasonable grounds to believe that evidence of the offences or suspected offences of accessing and possessing child pornography would be found at the places specified in the ITO, these being, generally stated, computer equipment, programs and software and related items and documentation, personal items confirming identification and credit card records and photographs, slides and other such items. In doing so, I excise

paragraph 11(b) of the ITO from consideration regarding the charge of accessing child pornography during the period of January 1 – 15, 2006.

[102] The same principle of one intending the natural consequences of one's actions, as set out in ***Missions***, applies. If Mr. Cafferata applied for access to a child pornography website and there is a credit card transaction showing a receipt of payment for this access, then the logical inference is that he was granted access to the website, that he did in fact access the site, and that proof of such access would be found in the places specified in the ITO. While this is not sufficient evidence to prove that Mr. Cafferata actually committed the offences with which he has been charged, it is enough to give Sgt. Johnson the reasonable grounds that he required to obtain the Search Warrant.

[103] I recognize that the evidence before me is less than it was in the ***Payne*** case, and I note that the credit card records were obtained in that case through subpoena, in that the investigative authorities in ***Payne*** did have further confirmation of an approval of membership, a login and password, prior to obtaining the Search Warrant. However, I also note that the court in ***Payne*** stated that when all the facts were considered in combination, these facts "…clearly supported a reasonable inference that the Defendant, in fact, subscribed to Illegal.CP". The use of the word "clearly" takes the consideration of the court beyond the evidence being "barely" enough.

[104] As such I am satisfied that the issuing judge had reasonable grounds such that he could have issued the Search Warrant.

Paragraph 11(b)

[105] I make the following comments regarding the potential application of the Canadian Adsoft Transaction.xls spreadsheet in paragraph 11(b) of the ITO to the evidence required to justify the issuance of the Search Warrant. It clearly cannot be used for the purpose for which it was originally placed before the

issuing judge. That said, there was evidence from Sgt. Johnson that amplified the meaning of and corrected the erroneous information. I have accepted that the error in including this information for its original stated purpose was simply an error with no attempt to mislead the authorizing justice and the authorizing judge. This nature of the error is relevant in assessing whether the issuing judge could have issued the Search Warrant, subject to accepting it as being reliable information. See ***R.*** v. ***Araujo***, [2000] 2 S.C.R. 992, at para. 57.

[106] I understand defence counsel's concerns about the lack of specific information surrounding how this spreadsheet was created. There is no start date and end date on an intercept for example. Sgt. Johnson testified that Sgt. Riccitelli told him that this information was information related to Adsoft that came from follow up search warrants and intercepts throughout their investigation.

[107] Given that this information came from the same US investigative authorities in the context of the same investigation detailed in the ITO, I am not prepared to consider it unreliable simply because I do not have the specific details as to exactly how it came about, such as which intercept and for which dates. As such, I consider this evidence reliable enough to include it in consideration with respect to reviewing whether the authorizing judge could have issued the Search Warrant.

[108] While it would be a stretch to put much weight, if any, on the April, 2006 confirmation of acceptance being proof of accessing child pornography in January, 2006, as this would require "reading backwards" to what happened or may have happened, it would appear, however, to place Mr. Cafferata in the position of potentially possessing child pornography within the prescribed dates of January 1, 2006 to September 4, 2007, for the same reasons set out above on the basis of the principle in ***Missions***. See also ***Payne***, at p. 13 where the court stated that it: "…'neither strains logic nor defies common sense' to conclude that an individual who pays $79.99 for a subscription to a child pornography website

has done so because he intends to view and download its content". This would then assist in providing reasonable grounds to believe that evidence regarding the offence or suspected offence of possessing child pornography would be found in the places specified in the ITO.

[109] Although I have not considered the information in paragraph 11(b) of the ITO as necessary for me to find that the authorizing Judge could have issued the Search Warrant, it remains nonetheless a further factor to support upholding his decision to do so.

[110] For all the reasons set out above, Mr. Cafferata has failed to demonstrate that his rights under s. 8 of the *Charter* were violated and I find that the Production Order and the Search Warrant were properly authorized in law.

Cozens T.C.J.