SUPREME COURT OF NOVA SCOTIA
Citation: *R. v. Fardy*, 2023 NSSC 28

Date: 20230125
Docket: CRK-507778
Registry: Kentville

Between:

His Majesty the King

v.

Jakob M. Fardy

DECISION ON SECTION 8 APPLICATION

Restriction on Publication: By court order made under subsection 486.4 of the *Criminal Code*, information that may identify the person described in this decision as the complainant may not be published, broadcasted or transmitted in any manner.

Judge:	The Honourable Justice Joshua Arnold
Heard:	November 8, 2022, in Kentville, Nova Scotia
Counsel:	Robert Kennedy and Erica Koresawa, for the Crown Zeb Brown, for Jakob Fardy

Order restricting publication - sexual offences

486.4 (1) Subject to subsection (2), the presiding judge or justice may make an order directing that any information that could identify the victim or a witness shall not be published in any document or broadcast or transmitted in any way, in proceedings in respect of

(a) any of the following offences:

(i) an offence under section 151, 152, 153, 153.1, 155, 160, 162, 163.1, 170, 171, 171.1, 172, 172.1, 172.2, 173, 213, 271, 272, 273, 279.01, 279.011, 279.02, 279.03, 280, 281, 286.1, 286.2, 286.3, 346 or 347, or

(ii) any offence under this Act, as it read from time to time before the day on which this subparagraph comes into force, if the conduct alleged would be an offence referred to in subparagraph (i) if it occurred on or after that day; or

(b) two or more offences being dealt with in the same proceeding, at least one of which is an offence referred to in paragraph (a).

Mandatory order on application

(2) In proceedings in respect of the offences referred to in paragraph (1)(a) or (b), the presiding judge or justice shall

(a) at the first reasonable opportunity, inform any witness under the age of eighteen years and the victim of the right to make an application for the order; and

(b) on application made by the victim, the prosecutor or any such witness, make the order.

Overview

[1] During the course of his arrest for multiple sexual assault and assault charges, RCMP officers seized Jakob Fardy's Apple iPhone. An ITO was subsequently prepared and a search warrant was issued for certain contents of Mr. Fardy's smartphone. The Crown wants to rely on various items of electronic evidence retrieved from Mr. Fardy's phone by police.

[2] At the commencement of trial, Mr. Brown, who represents Mr. Fardy, advised the court that he was challenging the constitutionality of the search on the basis that on its face the ITO did not set out reasonable grounds; the manner of the search went beyond what the search warrant authorized; the police scoured and/or "rummaged around" in Mr. Fardy's phone unconstitutionally; and the police failed to keep detailed notes of their search of the phone. As a result, he says that Mr. Fardy's s. 8 *Charter* rights were violated, and any evidence seized from his phone should be excluded under s. 24(2) of the *Charter of Rights and Freedoms*. The parties have asked for a decision on the s. 8 issue prior to making submissions regarding s. 24(2).

Facts

The ITO

[3] The Information to Obtain was sworn on September 16, 2020. It was drafted by Constable Christopher Robert Marshall who stated that he had been a member of the RCMP since July 2011, and that as of September 16, 2020, he had been involved in a variety of criminal investigations and had drafted no less than 95 ITOs.

[4] The items the affiant sought to search and seize are detailed at the outset of the ITO:

> **Data located a cellular device including:**
>
> - Messages (SMS, MMS, etc.)
> - Call logs
> - Social Media Application Messages (Facebook, Instagram, etc.)
> - Pictures

- Videos
- Emails

[5] I have reviewed and considered the entire ITO. Very generally, it includes a review of the charges facing Mr. Fardy, which involve allegations of assault and sexual assault respecting multiple complainants over the span of approximately four years. As of the writing of the ITO, the police had identified five complainants and had interviewed over 40 people. They had more people to interview, and had arrested and charged Mr. Fardy on July 30, 2020. The relevant passages of the ITO include the following:

> 5. …Mr. Fardy is an adult, of similar age to the victims and was either acquaintances of or dating the victims at the time of the assaults and sexual assaults…
>
> …
>
> **GROUNDS FOR RELIEF**
>
> 8. On July 15th, 2020, five (5) young women attended the New Minas RCMP Detachment to speak to police about having all been sexually assaulted by one male, Mr. Jakob Fardy. Statements were obtained from four of the young women and one woman was referred to the Kentville Police Services, as the sexual assault occurred in their area of jurisdiction. The following is a summary of what each of the four women said in their statements, these summaries have been placed in chronological order that the incidents took place for the reviewing Justice's ease of reading:
>
> **a. Police File #: 2020973139 – Ms. R.B.**
>
> i. Assault
>
> 1. On the night of March 17th , 2017, she was at a St. Patrick's Day party in Lakeville at Cole Butt's residence;
> 2. Two males got into an altercation at the party, one being a Mr. Aaron Cameron;
> 3. She stepped into the middle of the fight to break it up;
> 4. Mr. Fardy had been in a vehicle with another person, got out of the vehicle and said "where's my fucking girlfriend";
> 5. She and Mr. Fardy were dating at the time;
> 6. Mr. Fardy found her, grabbed her by the throat and dragged her over by Mr. Cameron's truck;

7. Mr. Fardy told her that she was "fucking disgusting" and she cried.

ii. Sexual Assault & Assault

1. Between the 25th of March and the 5th of April, she and Mr. Fardy were staying at Mr. Fardy's mother's home in Coldbrook;
2. The couple were being intimate and Mr. Fardy got up and pulled her over to the side of the bed;
3. Mr. Fardy asked her to perform oral sex on him;
4. She said no;
5. Mr. Fardy said "you're supposed to do this, you're my girlfriend";
6. Mr. Fardy grabbed hold of her head and kept trying to push it down towards his penis;
7. She would push away from Mr. Fardy;
8. She yelled at him to stop because she was scared and he kept pulling her closer to him;
9. Mr. Fardy almost had her pinned down on her side at this point;
10. Mr. Fardy got super angry and started yelling at her;
11. She kept telling him that she didn't want to give him oral sex;
12. She got scared and called one of her friends to come and get her;
13. Mr. Fardy overheard her conversation and told her that she needed to "get the fuck out of here" and to "shut the fuck up";
14. When she walked towards Mr. Fardy, he grabbed her by both wrists and flung her on the floor;
15. Mr. Fardy pinned her down and she was on the phone while this was happening;
16. Mr. Fardy wouldn't get off of her but eventually did;
17. She picked her phone up, hung up on her friend and left, and she never went back.

b. Police File #: 2020972901 – Ms. E.L.

i. Sexual Assault

1. On May 12th, 2017, Ms. L. received a message from Mr. Fardy asking if she wanted to go to a party with him;
2. Ms. L. had never hung out with him before but she agreed to go and Mr. Fardy picked her up;
3. The party was up the road from Mr. Fardy's mother's home in Coldbrook;
4. While at the party, Ms. L. got really really drunk and she blacked out;
5. Mr. Fardy took her home to his mother's place;
6. When she woke up the next morning, Mr. Fardy was on top of her and his penis was inside of her;
7. Mr. Fardy told her that she was his now and then he would choke her and hit her while continuing to have sex with her;
8. She told him to stop and began crying and she wound up going mute;
9. It was at this point that Mr. Fardy stopped and drove her home;
10. On the drive home Mr. Fardy got a ticket for speeding;
11. She never consented to any of the sexual acts Mr. Fardy performed on her.

c. Police File #: 2020973077 – Ms. C.O.

i. Sexual Assault

1. On June 15th, 2017, Ms. O. had a party at her home in Avonport which a large group of people attended;
2. Ms. O. was drinking wine during the party;
3. She began to feel the effects of the alcohol and she began dancing and kissing Mr. Aaron Cameron at around 10:00pm;
4. Mr. Cameron and her had consensual sex next to a tree behind the barn that the party was taking place in;
5. After having sex, she returned inside the barn and spoke with a few people before blacking out;

6. She woke up later that night on the love seat in the barn that the party had occurred in;
7. Mr. Fardy's penis was inside of her when she woke up, she was laying on her back with one of her legs and arms hanging off the love seat;
8. Mr. Fardy was leaning into her having sex with her;
9. She began crying and Mr. Fardy began apologizing for having "whiskey dick" as he was having difficulty continuing to penetrate her;
10. Mr. Fardy then laid down on her and continued to have sex with her until he fell asleep;
11. Once asleep, she managed to roll out from under Mr. Fardy and cried herself to sleep in an armchair;
12. The following morning Mr. Fardy thanked her for a good night and left with a friend.

d. Police File#: 2020972659 – Ms. J.M.

i. Sexual Assault

1. On March 27th, 2020, Ms. M. was home with Mr. Fardy, whom she was dating at the time, and two of her friends, Ms. N.T. and Ms. L.M.;
2. Mr. Fardy was drinking a quart of whiskey that night;
3. Mr. Fardy was belligerent and hurling insults at Ms. M. and her friends all evening;
4. Mr. Fardy then called Ms. M.'s ex-boyfriend, Mr. T.O., and challenged him to a fight;
5. Ms. M. tried to get Mr. Fardy to go to sleep as he had to work the next morning:
6. Ms. M. and Ms. T. went to sleep in their room and Ms. M. went to sleep in the room she shared with Mr. Fardy;
7. Mr. Fardy was in the room and ended up sitting up on the edge of the bed where he began masturbating;
8. Ms. M. asked Mr. Fardy what he was doing and he replied "just jerking it";
9. She asked him why he was doing that and he told her "because it just felt right";

10. She told him to go to sleep and it was at this point that Mr. Fardy climbed on top of her;

11. She told him to stop it and Mr. Fardy said "you are going to get fucked whether you like it or not" and Mr. Fardy then held her down with his forearm across Ms. M.'s chest;

12. Ms. M. began crying and told Mr. Fardy to stop;

13. This went on for about 10 minutes;

14. Once Mr. Fardy finished, he rolled over and went to sleep;

15. Ms. M. cried all night until Mr. Fardy got up to go to work a few hours later.

9. **a. Police File #: 2020977101 – Ms. S.M.**

i. Sexual Assault

1. Between the 25th day of May and the 10th day of June, 2016, Ms. M. was at a friend's house on Main Street in Kentville;

2. The friend that she was visiting was Mr. I.L. and also present was Mr. L.'s roommate, Mr. T.P. and Mr. P.'s girlfriend, Ms. T.S.;

3. Also present at the home that night was Mr. Fardy;

4. The group was partying and drinking and she got pretty drunk;

5. She went upstairs to Mr. L.'s bedroom and slept for at least an hour;

6. She was awoken by having pain and when she came to, she realized that Mr. Fardy was having sex with her from behind;

7. She was awake long enough to see Mr. Fardy's face and to feel that he was penetrating her vagina with his penis before she blacked out again;

8. When she woke up the night morning, Mr. Fardy was gone;

9. She contacted Mr. Fardy via text or snapchat and asked him what had happened the night before and said that she knew the gist of what had occurred;

10 . Mr. Fardy replied by saying "I was too high and horny".

Police File#: 2020972659 – Ms. J.M.

Ms. N.T. – interviewed by myself

1. During the initial stages of the COVID pandemic, she was living with Ms. M.;
2. Their friend, Ms. L.M. was also living with them
3. Mr. Fardy, who was dating Ms. M. at the time was also staying with them;
4. Mr. Fardy liked his whiskey and was drinking whiskey that night;
5. Mr. Fardy was saying offside things to Ms. M.;
6. Mr. Fardy later got upset about seeing Ms. M.'s ex's name, Mr. T.O., come up on his phone.
7. Mr. Fardy went downstairs and messaged Mr. O. challenging him to a fight.
8. She went downstairs to try to calm Mr. Fardy down;
9. Initially Mr. Fardy settled down but a short time later he was playing music loudly;

…

Mr. T.O. – interviewed by myself

…

4. He was at a friend's house minding his own business when at 2:45am he received a message from Mr. Fardy;
5. He messaged Mr. Fardy back asking him to call him if he wanted to talk;
6. Mr. Fardy never responded so he called Mr. Fardy;
7. He could barely understand Mr. Fardy on the phone as his speech was heavily slurred;
8. Eventually he could hear two female voices on the phone and the line went dead;
9. He wanted to go kick Mr. Fardy's ass but he thought better of it;
10. He received a call a short time later from Ms. M. accusing him of provoking Mr. Fardy;
11. He plead his case and eventually sent them a screenshot showing that Mr. Fardy had contacted him first;

12. He also had contact with Ms. M. the night that she broke up with Mr. Fardy in May;

…

12. On July 30th, 2020, at 9:45am, Cst. Whiteway received a phone call from Mr. Fardy who stated that he would not be attending the Detachment as previously agreed. Mr. Fardy stated that he had spoken with a lawyer and because he had done nothing wrong, he did not have to attend the Detachment. Cst. Whiteway explained to Mr. Fardy that he was going to be arrested for the allegations made against him and that police were trying to extend him the courtesy and dignity of attending the Detachment to deal with the matters instead of having the police come and look for him and arrest him at home, his place of work or anywhere else. Mr. Fardy was then told to contact his lawyer again and to call back once he had spoken to him.

13. A short time later, Mr. Fardy called back and indicated that after speaking to his lawyer, he would attend the Detachment to be arrested. Mr. Fardy advised that he would be at the Detachment shortly.

…

15. After his phone call with Mr. Conway, Mr. Fardy was booked into cells and his personal effects were put in a tray for safekeeping during his stay. Mr. Fardy's Apple iPhone, that was on his person at the time of his arrest, was seized from his personal effects as part of the investigation. As Cst. Whiteway was seizing the iPhone, it vibrated and the screen turned on. Cst. Whiteway noted three text messages from an "Aaron", who Cst. Whiteway believed to be Mr. Aaron Cameron. The messages were to the effect of "innocent until proven guilty", "don't say a fucking word" and "we're gonna get you through this". Mr. Fardy was secured in cells for a short period of time while members prepared to interview him. Mr. Fardy's iPhone was sealed in an exhibit bag and placed in a temporary exhibit locker until it could be taken to RCMP Headquarters in Dartmouth to be secured in the Tech Crime Unit's exhibit locker.

…

SUMMARY

24. Based on the information provided in this affidavit, I have reasonable grounds to believe the following:

a. That Mr. Fardy sexually assaulted five different women during a period of 4 years and assaulted two of the same victims during that same time frame;

b. That Mr. Fardy committed two of the sexual assaults and all three assaults in the context of domestic violence as he was dating one of the

victim's and dating and living with the other victim at the time of the offences;

c. That Mr. Fardy communicated with his victims via cellular phone including text messages and social media applications. This belief is based on the statements provided by the victims and the fact that Mr. Fardy was dating two of the victims and it would be reasonable to believe that Mr. Fardy communicated with both victims, Ms. B. and Ms. M., via cellular phone during their relationships;

d. That Mr. Fardy was in possession of a cellular phone at the time of his arrest;

e. That Mr. Fardy received text messages, that are relevant to the matters at hand, from a friend during the processing of his personal effects by the arresting officers;

…

25. Based on the information provided in this affidavit, I have reasonable grounds to believe that a search of the following would provide evidence in respect of the offence being investigated:

a. Based on my experience as a police officer and my own personal experiences in communicating with my spouse, my friends, my colleagues and my family, that in society today, we are constantly connected to our phones and we are in constant communication with others;

b. Mr. Fardy would have been in communication with the victims or with other people around the time of the offences via his cellular phone;

…

d. Mr. Fardy was in possession of an Apple iPhone at the time of his arrest and he received text messages from a friend directed to him that are relevant to these matters;

e. The above noted date ranges have been sought as they are inclusive of the offence date plus 90 days from the date that the offence occurred in each circumstance. The offences in 2017 all occurred within a few months of each other and the final offence occurred in May 2017. These date ranges are being sought to capture any communications that occurred between Mr. Fardy and anyone else, after the offences occurred, but are limited to these short windows so as not to be overly broad.

26. Currently the RCMP H Division Technological Crime Unit is the only unit in the Province of Nova Scotia with the ability to search electronic devices. Due to their workload, their unit may require up to six months before being able to search the electronic device. [As appears in original]

Blended Voir Dire Evidence

[6] As noted above, in addition to attacking the ITO on its face, Mr. Fardy also says the search was overbroad and therefore unconstitutional. The warrant did not authorize the police to search his internet history, yet the police seized that information from his phone.

[7] The Crown concedes that there was no judicial authorization to search and seize the internet history, but says that since they are not relying on this information it has no bearing on the constitutionality of the search.

[8] Crown and defence advised the court that they wanted to proceed by way of a blended *voir dire*, as Mr. Fardy originally took the position that if his s. 8 *Charter* challenge was unsuccessful, the evidence taken from his phone would be inadmissible in any event. In this case the term "blended *voir dire"* refers to the attack on the ITO on its face; hearing evidence related to the manner of the search; whether the search was overbroad; whether the Crown requires an expert to give evidence about the cell phone extraction; and whether the evidence of the cell phone extraction can be properly authenticated.

[9] Mr. Fardy said the evidence regarding the extraction of the cell phone contents requires expert testimony, and pointed out that the Crown did not provide a Notice of Expert in advance of trial as mandated under the *Criminal Code*. The Crown said no expert is required to tender the evidence extracted from the cell phone.

[10] Mr. Fardy also said the cell phone evidence is inadmissible because it cannot not be properly authenticated. According to him, the programs used to extract the evidence from the phone (Cellebrite and Graykey) have not been proven to be reliable. The Crown disputed this position.

[11] Following the blended *voir dire*, Crown and defence came to an agreement regarding the expert evidence and authentication issues. They agree that these issues are now moot and no longer seek rulings.

[12] The sole issue remaining is whether s. 8 of the *Charter* was violated. Mr. Fardy is attacking the ITO on its face, and the Crown did not offer amplification. After the hearing, both parties asked me to consider selected *viva voce* evidence heard on the blended *voir dire* on the issue of the manner of the search, that is, the allegations of scouring and/or rummaging through the phone, as well as the issue of lack of police note-taking during the search.

[13] In correspondence dated November 14, 2022, defence counsel detailed the evidence he says is relevant to the manner of the search, in respect of each of the two witnesses called on this blended *voir dire*:

> With respect to the evidence on the s. 8 voir dire, in addition to the warrant and ITO, the following are relevant in regard to manner of search:
>
> Glen MacKenzie:
>
> - exported and provided all categories of data to the investigator, including location history, website searches, device logs, account details, etc.
> - demonstrated that the user interface for selecting categories of data is clear and easy to use, i.e. simply check or uncheck the boxes for each type of data
> - he could have overlooked the specified categories of data on the warrant when he exported the data
> - no evidence of any safeguard to prevent overbroad export of private data
>
> Cpl Chris Marshall:
>
> - he never reviews the warrant after receiving the data but in hindsight he should have done so
> - did not keep detailed notes of what he reviewed, he only noted what he found interesting or possibly relevant
> - he reviewed or scanned through every message of every conversation
> - no evidence of any precautions to avoid breaching solicitor/client privilege

[14] In correspondence dated November 14, 2022, the Crown asked me to consider the following *viva voce* evidence heard on the blended *voir dire* in relation to the manner of the search:

> Section 8 – Facial Validity of ITO
>
> Exhibit 1 – Search Warrant dated September 16, 2020
>
> Exhibit 2 – ITO dated September 16, 2020
>
> Section 8 – Overbroad Manner of Search
>
> Exhibit 4 – UFDR Report (2020)

Glen MacKenzie

Direct Examination:

- In this case, he was asked to provide UFDR reports with different date ranges.
- Exhibit 4 is the UFDR for the 2020 date ranges
    - When you open the program, you get the home page
    - He created 3 UFDR Reports
    - Exhibit 4 is a copy of the 2020 UFDR Report
    - Two Apple IDs detected on this device – both bearing the name of the accused
    - Apple ID is "Jakob's iPhone"
    - Unique ID on extraction reports is specific to the device
    - Serial number of SIM Card on home page of UFDR matches the SIM card that was taped to the back of the phone
    - Phone number for phone is 902-300-6117
    - "Case Information" on home page of UFDR is automatically created by Cellebrite. The only things manually entered is the examiner name and case name
- Cellebrite parses the extraction and returns it
- Walks through extraction
    - Used trusted forensic tool (Graykey)
    - Graykey plugs into device and into a monitor. If it detects the device, it determines whether it can extract anything
    - The interface opens on a monitor. It is menu-driven.
    - The program goes through options of what it can extract
    - He then copies the extraction from Graykey to the PC and loads it into Cellebrite Physical Analyzer
- Once forensic image has been made, he opened it on PC in Cellebrite Physical Analyzer
    - The looked at the warrant for type of data/dates
    - Then he went through the report menu
    - He doesn't look or sift through evidence

    - UFDR reports are subsets of the main extraction
- Exhibit 4 (2020 UFDR) – there is a list on the left, you click on "Analyzed Data" which shows various types of data, including media, messages etc.
    - The program itself automatically extracts this data
    - This report covers March to July 2020 (dates from the warrant)
- Exhibit 1 (warrant), there is a list of 6 types of data
    - These items are covered by Exhibit 4 (2020 UFDR), but there are other items in Exhibit 1 that are not covered by warrant because Exhibit 1 is the whole shell of the extraction. If a box is not unselected, it would be included in the UFDR. This could have been an oversight in this case.
- In this case, he received the phone from the evidence locker. He took photos of the phone. He looked at the condition of the device and did manual verification
- With a full extraction report, if there is any explicit content (child exploitation etc.), then he will advise the investigator and encrypt that data
- The UFDRs are provided to the investigator
- He doesn't identify evidence contained in the extraction or UFDRs
- If the investigator has issues with navigating the report, he can make himself available to walkthrough the report(s), but some don't need it
- Intimate images were vetted at the request of the investigator
- When UFDR is created, he only does a cursory look to ensure that something populates

<u>Cross-Examination:</u>

- Exhibit 3 – the data should only pertain to March to July 2020 date range
- He doesn't know how the program decides if "user accounts" or something else that doesn't have a date range are included in extraction
- When you create a report, you get an option of "Data Types" to check on
- He was asked why all of the data types listed under "Analyzed Data" of Exhibit 4 went to the investigator. He stated that it was an oversight. He doesn't know if you can take certain things out – for example, "configurations". He also doesn't know if "user accounts" can be turned off" but shows that it can be physically unclicked.
- He created 3 UFDR reports and provided them to the investigator. Prior to sending them to the investigator, Cpl. Marshall came to the DFS office to

do an initial review. He set up Marshall at a reviewing station and provided the UFDRs.

- He doesn't recall if Marshall looked at the main extraction or the 3 UFDR reports.

Cpl. Marshall

Direct Examination:

- Fardy was arrested on July 30, 2020. Fardy had an iPhone in his possession. It was turned over to Cst. Whiteway from Fardy's pocket.
- He drafted the ITO to search this phone. September 16, 2020.
- The warrant to search the phone was approved. The phone was already in DFU's evidence locker.
- He filled out a form requesting that DFU conduct extraction. He provided the form to his supervisor who approved it. A copy of the form and the warrant were forwarded to Tech Crime.
- The form includes a brief overview, file number, name of the accused, court dates, if there was a passcode and the type of device
- The warrant authorized messages, call logs, social media apps, pictures, videos and emails to be searched
- The date ranges contained in the warrant included the offences dates and 90 days thereafter:
    - May 25 to August 25, 2016
    - March 17 to August 17, 2017
    - March 27 to July 30, 2020
- DFU contacted him in early November 2020 to advise that data was ready to be reviewed
- On November 5, 2020, he attended DFU and did an initial review of the data
    - It was quick, not lengthy. He made some notes about things that seemed relevant to the investigation
- He only reviewed the UFDRS within the date ranges of the warrant
- He reviewed texts – he was primarily focussed on any messaging, call logs, web search history, pictures and videos
    - This was during the initial review

  - A lot of conversations didn't seem relevant
  - He didn't look at any other types of data
- On November 12, 2020, he was able to dig a little deeper. He found things that he thought were relevant. He created PDF reports of text conversations
  - He didn't look at any other types of data outside of the warrant this day either
- He acknowledges that "web history' is not listed in the warrant. He explains that in any other investigation prior to this one, he's only given the data available on the face of the data. He hadn't reviewed the warrant again before reviewing the UFDRs. Every time he write warrant for phones in the past, he only got the data that he requested.
- When looking at pictures/videos, he noted intimate images. He noted that vetting was required. Another officer took this over, as Marshall was moving onto new role in RCMP.
- His objective when searching the UFDRs was to find any conversations between the accused and the victims or witnesses already identified and any others who were family/friends of the victims or the accused. He ignored things that seemed entirely irrelevant.

Cross-Examination:

- This was his 95th judicial authorization
- He made handwritten notes that are in disclosure
- His notes included the particular text conversation and the name so he could go back and review
- Notes would have referenced how long the search was – 1-2 hours, maybe more
- He didn't list all the data looked at, just what was of note
- It is not possible that he reviewed other types of data but not noted. He recalls scrolling through the things that he did

Law in relation to s. 8 of the *Charter* and Search Warrants

Section 487 of the Criminal Code:

[15] Section 487 of the *Criminal Code* states:

> **487 (1)** A justice who is satisfied by information on oath in Form 1 that there are 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 will reveal the whereabouts of a person who is believed to have committed an offence, against this Act or any other Act of Parliament,
> >
> > …
> >
> > may at any time issue a warrant authorizing a peace officer or a public officer who has been appointed or designated to administer or enforce a federal or provincial law and whose duties include the enforcement of this Act or any other Act of Parliament and who is named in the warrant
> >
> > **(d)** to search the building, receptacle or place for any such thing and to seize it, and
> >
> > **(e)** subject to any other Act of Parliament, to, as soon as practicable, bring the thing seized before, or make a report in respect thereof to, the justice or some other justice for the same territorial division in accordance with section 489.1.

Breadth of s. 487

[16] In *CanadianOxy Chemicals Ltd. v. Canada (Attorney General)*, [1999] 1 SCR 743, Major J., for the unanimous court, explained the need for a broad interpretation of s. 487 in the context of the purpose of a criminal investigation:

> 20 A primary, though not exclusive, purpose of the *Criminal Code*, and penal statutes in general, is to promote a safe, peaceful and honest society, This is achieved by providing guidelines prohibiting unacceptable conduct, and providing for the just prosecution and punishment of those who transgress these norms. The prompt and comprehensive investigation of potential offences is essential to fulfilling that purpose. The point of the investigative phase is to gather all the relevant evidence in order to allow a responsible and informed decision to be made as to whether charges should be laid.
>
> 21 At the investigative stage the authorities are charged with determining the following: What happened? Who did it? Is the conduct criminally culpable behaviour? Search warrants are a staple investigative tool for

answering those questions, and the section authorizing their issuance must be interpreted in that light.

22 The purpose of s. 487(1) is to allow the investigators to unearth and preserve as much relevant evidence as possible. To ensure that the authorities are able to perform their appointed functions properly they should be able to locate, examine and preserve all the evidence relevant to events which may have given rise to criminal liability. It is not the role of the police to investigate and decide whether the essential elements of an offence are made out – that decision is the role of the courts. The function of the police, and other peace officers, is to investigate incidents which might be criminal, make a conscientious and informed decision as to whether charges should be laid, and then present the full and unadulterated facts to the prosecutorial authorities. To that end an unnecessary and restrictive interpretation of s. 487(1) defeats its purpose. See *Re Church of Scientology and the Queen (No. 6)* (1987), 31 C.C.C. (3d) 449, p. 475:

> Police work should not be frustrated by the meticulous examination of facts and law that is appropriate to a trial process. . . . There may be serious questions of law as to whether what is asserted amounts to a criminal offence. . . . However, these issues can hardly be determined before the Crown has marshalled its evidence and is in a position to proceed with the prosecution.

23 Moreover, extrinsic factors such as the accused's motive or the failure to exercise due diligence are often relevant to determining whether the event which triggered the investigation in the first place is criminally culpable. Everyone, including accused persons, who lacks the means of obtaining and preserving evidence prior to trial has an interest in seeing that these facts are brought to light. It would be undesirable if a narrow reading of s. 487(1) resulted in either inculpatory or exculpatory evidence being lost because of the investigators' inability to secure it. See *R. v. Storrey*, [1990] 1 S.C.R. 241, *per* Cory J., at p. 254:

> The essential role of the police is to investigate crimes. That role and function can and should continue after they have made a lawful arrest. The continued investigation will benefit society as a whole and not infrequently the arrested person. It is in the interest of the innocent arrested person that the investigation continue so that he or she may be cleared of the charges as quickly as possible.

> 24 It is important that an investigation unearth as much evidence as possible. It is antithetical to our system of justice to proceed on the basis that the police, and other authorities, should only search for evidence which incriminates their chosen suspect. Such prosecutorial "tunnel vision" would not be appropriate…

[17] Recognizing the need to balance this broad power to search against privacy concerns, Major J. continued:

> 28 There is no doubt that search warrants are highly intrusive, and that an investigation bearing on the issue of due diligence could, as Shaw J. pointed out in *Re Domtar*, *supra*, at p. 119, "entail a detailed inquiry into the affairs of a corporation over a period of several years". This Court has endorsed the importance of privacy and the need to constrain search powers within reasonable limits…
>
> > 29 The broad powers contained in s. 487(1) do not authorize investigative fishing expeditions, nor do they diminish the proper privacy interests of individuals or corporations. This is particularly true with respect to personnel records which may contain a great deal of highly personal information unrelated to the investigation at hand. Judges and magistrates should continue to apply the standards and safeguards which protect privacy from unjustified searches and seizures.
>
> 29 In this case, however, the specific terms of the warrant were not at issue, as the respondents challenged only the underlying authority to grant warrants for the purpose of investigating the presence of negligence. In our opinion both a plain reading of the relevant section and consideration of the role and obligations of state investigators support the conclusion that s. 487(1) authorized the granting of the warrants at issue.

Search of computers and mobile phones

[18] The Supreme Court of Canada has issued the strongest of cautions when it comes to the state listening to private citizens' conversations or searching their computers and mobile phones. It is against this background that the search of Mr. Fardy's Apple iPhone must be considered.

[19] In relation to wiretaps of private citizens' telephone conversations, in *R. v. Araujo*, [2000] 2 SCR 992, LeBel J., for the court, explained the need to protect privacy and to balance that against the need for effective law enforcement:

> 21 The meaning of the investigative necessity requirement is of critical importance by reason of the conflict between the privacy interests involved in wiretapping operations and the needs of law enforcement agencies in their difficult fight against some forms of sophisticated and dangerous criminality. Wiretapping is highly intrusive. It may affect human relations in the sphere of very close, if not intimate communications, even in the privacy of the home. La Forest J. was alert to the importance of the societal values involved in wiretapping and the risks to essential privacy interests. Writing for the Court, in *Duarte*, *supra*, at p. 44, La Forest J. emphasized the potential danger to privacy rights arising from the use of such modern investigative techniques:
>
> > The reason for this protection is the realization that if the state were free, at its sole discretion, to make permanent electronic recordings of our private communications, there would be no meaningful residuum to our right to live our lives free from surveillance. The very efficacy of electronic surveillance is such that it has the potential, if left unregulated, to annihilate any expectation that our communications will remain private. A society which exposed us, at the whim of the state, to the risk of having a permanent electronic recording made of our words every time we opened our mouths might be superbly equipped to fight crime, but would be one in which privacy no longer had any meaning. As Douglas J., dissenting in *United States v. White*, *supra*, put it, at p. 756: "Electronic surveillance is the greatest leveler of human privacy ever known". If the state may arbitrarily record and transmit our private communications, it is no longer possible to strike an appropriate balance between the right of the individual to be left alone and the right of the state to intrude on privacy in the furtherance of its goals, notably the need to investigate and combat crime.

[20] Ten years later, when considering state intrusion into personal computers, Fish J. recognized the resulting privacy concerns in *R. v. Morelli*, [2010] 1 SCR 253, where he said, for the majority*:*

> [105] As I mentioned at the outset, it is difficult to imagine a more intrusive invasion of privacy than the search of one's home and personal computer. Computers often contain our most intimate correspondence. They contain the details of our financial, medical, and personal situations. They even reveal our specific interests, likes, and propensities, recording in the browsing

> history and cache files the information we seek out and read, watch, or listen to on the Internet.
>
> …
>
> [109] In my view, the repute of the administration of justice will be significantly undermined if criminal trials are permitted to proceed on the strength of evidence obtained from the most private "place" in the home on the basis of misleading, inaccurate, and incomplete Informations upon which a search warrant was issued.
>
> [110] Justice is blind in the sense that it pays no heed to the social status or personal characteristics of the litigants. But justice receives a black eye when it turns a blind eye to unconstitutional searches and seizures as a result of unacceptable police conduct or practices.

[21] The court expanded on the need to recognize privacy interests when it comes to state intrusions involving personal computers in *R. v. Vu*, [2013] 3 SCR 657, where Cromwell J. stated, for the court:

> [24] The privacy interests implicated by computer searches are markedly different from those at stake in searches of receptacles such as cupboards and filing cabinets. Computers potentially give police access to vast amounts of information that users cannot control, that they may not even be aware of or may have chosen to discard and which may not be, in any meaningful sense, located in the place of the search. These factors, understood in light of the purposes of s. 8 of the *Charter*, call for specific pre-authorization in my view.

[22] Then, in *R. v. Fearon*, 2014 SCC 77, Cromwell J., for the majority, extended these privacy considerations to mobile phones (in the context of a search incident to arrest, not as authorized by a warrant). He said:

> [57] Third, the common law requirement that the search be truly incidental to a lawful arrest imposes some meaningful limits on the scope of a cell phone search. The search must be linked to a valid law enforcement objective relating to the offence for which the suspect has been arrested. This requirement prevents routine browsing through a cell phone in an unfocussed way.
>
> …
>
> [78] There is a parallel here with the Court's decision in *Vu*. A warrant to search a computer does not give the police "a licence to scour the devices indiscriminately": para. 61. Similarly, the fact that some examination of a cell phone is truly incidental to arrest does not give the police a licence to rummage around in the device at will. The nature and extent of the search must be truly incidental to the arrest in order for it to fall within the scope of the common law

> rule and respect s. 8 of the *Charter*. I agree with the courts of appeal in British Columbia and Nova Scotia that, generally, the search of the entire contents of a cell phone or a download of its contents is not permitted as a search incident to arrest: *Mann*, at para. 123; *Hiscoe*, at paras. 63 and 79.
>
> …
>
> [82] Finally, officers must make detailed notes of what they have examined on the cell phone. The Court encouraged this sort of note keeping in *Vu* in the context of a warranted search: para. 70. It also encouraged that notes be kept in the context of strip searches: *Golden*, at para. 101. In my view, given that we are dealing here with an extraordinary search power that requires neither a warrant nor reasonable and probable grounds, the obligation to keep a careful record of what is searched and how it was searched should be imposed as a matter of constitutional imperative. The record should generally include the applications searched, the extent of the search, the time of the search, its purpose and its duration. After-the-fact judicial review is especially important where, as in the case of searches incident to arrest, there is no prior authorization. Having a clear picture of what was done is important to such review being effective. In addition, the record keeping requirement is likely to have the incidental effect of helping police officers focus on the question of whether their conduct in relation to the phone falls squarely within the parameters of a lawful search incident to arrest. [Emphasis added]

[23] In extending privacy considerations and protection to text messages between mobile phone users, in *R. v. Marakah*, 2017 SCC 59, McLachlin C.J. said, for the majority:

> [32] In considering this factor, the focus is not on the actual contents of the messages the police have seized, but rather on the potential of a given electronic conversation to reveal personal or biographical information. For the purposes of s. 8 of the *Charter*, the conversation is an "opaque and sealed 'bag of information'": *Patrick*, at para. 32; see also *Wong*, at p. 50. What matters is whether, in the circumstances, a search of an electronic conversation may betray "information which tends to reveal intimate details of the lifestyle and personal choices of the individual" (*Plant*, at p. 293), such that the conversation's participants have a reasonable expectation of privacy in its contents, whatever they may be: see *Cole*, at para. 47; *Tessling*, at paras. 25 and 27.
>
> [33] Individuals may even have an acute privacy interest in the *fact* of their electronic communications. As Marshall McLuhan observed at the dawn of the technological era, "the medium is the message": M. McLuhan, *Understanding Media: The Extensions of Man* (1964), at p. 7. The medium of text messaging broadcasts a wealth of personal information capable of revealing personal and core biographical information about the participants in the conversation.

> [34] The personal nature of the information that can be derived from text messages is linked to the private nature of texting. People may be inclined to discuss personal matters in electronic conversations precisely because they understand that they are private. The receipt of the information is confined to the people to whom the text message is sent. Service providers are contracted to confidentiality. Apart from possible police interception — which cannot be considered for the purpose of determining a reasonable expectation of privacy (see *Patrick*, at para. 14; *Wong*, at p. 47; *R. v. Duarte*, [1990] 1 S.C.R. 30, at pp. 43-44) — no one else knows about the message or its contents.
>
> [35] Indeed, it is difficult to think of a type of conversation or communication that is capable of promising more privacy than text messaging. There is no more discreet form of correspondence. Participants need not be in the same physical place; in fact, they almost never are. It is, as this Court unanimously accepted in *TELUS*, a "private communication" as that term is defined in s. 183 of the *Criminal Code*, R.S.C. 1985, c. C-46, namely, "[a] telecommunication . . . that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted by any person other than the person intended by the originator to receive it": see *TELUS*, at para. 12, per Abella J., at para. 67, per Moldaver J., and at para. 135, per Cromwell J.
>
> [36] One can even text privately in plain sight. A wife has no way of knowing that, when her husband appears to be catching up on emails, he is in fact conversing by text message with a paramour. A father does not know whom or what his daughter is texting at the dinner table. Electronic conversations can allow people to communicate details about their activities, their relationships, and even their identities that they would never reveal to the world at large, and to enjoy portable privacy in doing so.
>
> [37] Electronic conversations, in sum, are capable of revealing a great deal of personal information. Preservation of a "zone of privacy" in which personal information is safe from state intrusion is the very purpose of s. 8 of the *Charter*: see *Patrick*, at para. 77, per Abella J. As the foregoing examples illustrate, this zone of privacy extends beyond one's own mobile device; it can include the electronic conversations in which one shares private information with others. It is reasonable to expect these private interactions — and not just the contents of a particular cell phone at a particular point in time — to remain private. [Emphasis added]

[24] More recently, in *R. v. Reeves*, [2018] 3 SCR 531, Karakatsanis J. for the majority, reiterated the need to recognize the highly intimate and personal information that can be found on a private computer:

> [34] Personal computers contain highly private information. Indeed, "[c]omputers often contain our most intimate correspondence. They contain the details of our financial, medical, and personal situations. They even reveal our

> specific interests, likes, and propensities" (*R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, at para. 105; see also *Vu*, at paras. 40-41; *Cole*, at paras. 3 and 47-48). Computers act as portals — providing access to information stored in many different locations (*Vu*, at para. 44; *R. v. Fearon*, 2014 SCC 77, [2014] 3 S.C.R. 621, at paras. 131-32). They "contain information that is automatically generated, often unbeknownst to the user" (*Vu*, at para. 42). They retain information that the user may think has been deleted (*Vu*, at para. 43). By seizing the computer, the police deprived Reeves of control over this highly private information, including the opportunity to delete it. They also obtained the means through which to access this information. Indeed, these are the reasons why the police seized the computer.
>
> [35] Given the unique privacy concerns associated with computers, this Court has held that specific, prior judicial authorization is required to search a computer (*Vu*, at para. 2) and that police officers cannot search cell phones incident to arrest unless certain conditions are met (*Fearon*, at para. 83). The unique and heightened privacy interests in personal computer data clearly warrant strong protection, such that specific, prior judicial authorization is presumptively required to seize a personal computer from a home. This presumptive rule fosters respect for the underlying purpose of s. 8 of the *Charter* by encouraging the police to seek lawful authority, more accurately accords with the expectations of privacy Canadians attach to their use of personal home computers and encourages more predictable policing.

[25] The police had prior judicial authorization to search Mr. Fardy's phone. The question is whether the ITO was sufficient, and whether the search went too far.

General framework for challenging the ITO

[26] According to s. 487 of the *Criminal Code*, in order for a search warrant to be issued the police must have reasonable grounds to believe that there is, in the receptacle to be searched, anything that there are reasonable grounds to believe in the receptacle or place anything on or in respect of which an offence has been or is suspected to have been committed, or anything that there are reasonable grounds to believe will afford evidence with respect to the commission of an offence.

[27] Reasonable grounds are made out when credibly-based probability replaces mere suspicion. The police officer's subjective grounds must be justified on an objective basis. A reasonable belief must be demonstrated and must amount to more than just a hunch or a suspicion on a practical, non-technical, common-sense

approach to the totality of evidence. As stated by Frankel J. in *R. v. Jir*, 2010 BCCA 497:

> [27] As has been stated many times, the "reasonable grounds" standard is not only less than that required for conviction, but is also less than the civil standard of proof. Madam Justice Wilson put it this way in *R. v. Debot*, 1989 CanLII 13 (SCC), [1989] 2 S.C.R. 1140 at 1166:
>
> > The question as to what standard of proof must be met in order to establish reasonable grounds for a search may be disposed of quickly. I agree with Martin J.A. that the appropriate standard is one of "reasonable probability" rather than "proof beyond a reasonable doubt" or "*prima facie* case". The phrase "reasonable belief" also approximates the requisite standard.
>
> More recently, in *Mugesera v. Canada (Minister of Citizenship & Immigration)*, 2005 SCC 40, [2005] 2 S.C.R. 100, the Court stated (at para. 114):
>
> > … the "reasonable grounds to believe" standard requires something more than mere suspicion, but less than the standard applicable in civil matters of proof on the balance of probabilities [citations omitted].
>
> Further, as Mr. Justice Hill noted in *R. v. Sanchez* (1994), 1994 CanLII 5271 (ON SC), 93 C.C.C. (3d) 357 at 367 (Ont. Ct. (G.D)):
>
> > 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.

[28] A search conducted under the authority of a judicial authorization is presumed to be valid *R v Pires; R v Lising*, 2005 SCC 66, at para 30. The onus is on the party challenging the warrant to establish that it is not valid on a balance of probabilities: *R. v. Cameron*, 2021 ONSC 2154, at para. 66.

[29] In *R. v. Araujo*, [2000] 2 S.C.R. 992, LeBel J. explained the limited role of a reviewing judge:

> 51 The reviewing judge does not stand in the same place and function as the authorizing judge. He or she does not conduct a rehearing of the application for the wiretap. This is the starting place for any reviewing judge, as our Court stated in *Garofoli*, *supra*, at p. 1452:
>
> > The reviewing judge does not substitute his or her view for that of the authorizing judge. If, based on the record which was before the authorizing judge as amplified on the review, the reviewing judge

> concludes that the authorizing judge could have granted the authorization, then he or she should not interfere**.** In this process, the existence of fraud, non-disclosure, misleading evidence and new evidence are all relevant, but, rather than being a prerequisite to review, their sole impact is to determine whether there continues to be any basis for the decision of the authorizing judge.

As I noted as a judge at the Quebec Court of Appeal in *Hiscock*, *supra*, at p. 326 C.C.C., even a basis that is schematic in nature may suffice. However, as our Court has recognized, it must be a basis founded on reliable information. In *R. v. Bisson*, [1994] 3 S.C.R. 1097, at p. 1098, the requirement was described as "sufficient reliable information to support an authorization" (emphasis added). The Court concluded that this requirement had still been met despite the excision of retracted testimony. In looking for reliable information on which the authorizing judge could have granted the authorization, the question is simply whether there was at least some evidence that might reasonably be believed on the basis of which the authorization could have issued.

…

54 The authorities stress the importance of a contextual analysis. The Nova Scotia Court of Appeal, while reviewing the cases from our Court cited above, explains this in a judgment dealing with problems arising out of errors committed in good faith by the police in the material submitted to the authorizing justice of the peace:

> These cases stress that errors, even fraudulent errors, do not automatically invalidate the warrant.
>
> This does not mean that errors, particularly deliberate ones, are irrelevant in the review process. While not leading to automatic vitiation of the warrant, there remains the need to protect the prior authorization process. The cases just referred to do not foreclose a reviewing judge, in appropriate circumstances, from concluding on the totality of the circumstances that the conduct of the police in seeking prior authorization was so subversive of that process that the resulting warrant must be set aside to protect the process and the preventive function it serves. [Emphasis added.]

(*R. v. Morris* (1998), 134 C.C.C. (3d) 539, at p. 553)

> An approach based on looking for sufficient reliable information in the totality of the circumstances appropriately balances the need for judicial finality and the need to protect prior authorization systems. Again, 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. [Emphasis added]

[30] Therefore, the scope of my review is narrow and does not constitute a *de novo* review of the *ex parte* application. My role as the reviewing judge is not to substitute my assessment of the evidence for that of the authorizing judge. As Fish J. stated in *Morelli*:

> [40] In reviewing the sufficiency of a warrant application, however, "the test is whether there was reliable evidence that might reasonably be believed on the basis of which the authorization could have issued" (*R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992, at para. 54 (emphasis in original)). The question is not whether the reviewing court would itself have issued the warrant, but whether there was sufficient credible and reliable evidence to permit a justice of the peace to find reasonable and probable grounds to believe that an offence had been committed and that evidence of that offence would be found at the specified time and place. [Emphasis added.]

[31] The authorizing justice is entitled to make reasonable inferences when determining whether the search warrant should issue and the informant need not underline the obvious. As stated by Cromwell J. in *R v Vu*, 2013 SCC 60:

> [16] The question for the reviewing judge 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": *R. v. Araujo*, 2000 SCC 65, [2000] 2 S.C.R. 992, at para. 54 (emphasis deleted); *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253, at para. 40. In applying this test, the reviewing judge must take into account that authorizing justices may draw reasonable inferences from the evidence in the ITO; the informant need not underline the obvious… [Emphasis added]

[32] Mere conclusory statements by the affiant are not enough. Facts must support the conclusions drawn, but the authorizing justice is able to nonetheless draw inferences. As Frankel J. noted in *Jir*:

> [37] In the case at bar, to paraphrase what Madam Justice Rowles said in *R. v. Ngo*, 2009 BCCA 301 at para. 60, the question is whether, on the whole of the

evidence, the trial judge could reasonably have concluded, beyond a reasonable doubt, that Mr. Jir knew of the drugs in the trunk of the Sebring. Also apt is the following from the judgment of Chief Justice McEachern in *R. v. To* (1992), 16 B.C.A.C. 223, a case in which this Court held that it was open to the trial judge to infer that Mr. To knew that the closed bag he was carrying contained several million dollars worth of drugs:

> 19 The first question is whether the evidence permitted the learned trial judge to conclude beyond a reasonable doubt that knowledge on the part of the accused was the only reasonable inference to be drawn from the proven facts: *R. v. Cooper* (1977), 34 C.C.C. (2d) 18 (S.C.C.) per Ritchie J. at p. 33.
>
> 20 In this respect, our function is not to second-guess the trial judge, but merely to examine the evidence, and consider whether the judge has correctly applied the law to the facts of the case. ...
>
> . . .
>
> 41 It must be remembered that we are not expected to treat real life cases as a completely intellectual exercise where no conclusion can be reached if there is the slightest competing possibility. The criminal law requires a very high degree of proof, especially for inferences consistent with guilt, but it does not demand certainty. I do not think it could properly be said that an inference of knowledge in this case would be unreasonable or unsupported by the evidence.

[33] In *R. v. Liu*, 2014 BCCA 166, the court provided a summary of the approach a reviewing judge should undertake when determining a facial review of an ITO

> [39] I would summarize the main points from this jurisprudence in the following way:
>
> - The trial judge's role in reviewing the validity of a search warrant is to consider whether the material filed in support of the warrant, as amplified on review, could support the issuance of the warrant.
>
> - The trial judge should examine the information in its totality, not on a piece meal basis, in a "practical, non-technical, and common sense basis".
>
> - The question is not whether the reviewing judge would have granted the order, but whether there was an objective basis on which the issuing justice could have done so.
>
> - The appropriate standard is one of "reasonable probability" rather than "proof beyond a reasonable doubt" or "*prima facie* case". The phrase "reasonable belief" also approximates the requisite standard.
>
> - Reasonable grounds may be said to exist at "the point at which credibly-based probability replaces suspicion".

[34] If the reviewing judge determines that the inferences drawn by the issuing judge are reasonable on the facts disclosed in the ITO, this demonstrates that the authorizing judge **could** have issued the warrant and the warrant should be upheld. Mr. Fardy has brought a facial challenge to the ITO on the sufficiency issue. The record on a facial review is fixed, involving a review of the ITO only. As noted above, there is no amplification of the record in this case.

[35] In relation to the meaning of s. 487(b), that is "will afford evidence with respect to the commission of an offence", Sharma J. discussed the interpretation of this phrase in *R. v. Abo Zead*, 2020 BCSC 1970:

> [39] The Supreme Court of Canada has commented on the meaning of the phrase in paragraph (b) above, "will afford evidence with respect to the commission of an offense", in *CanadianOxy Chemicals Ltd. v. Canada (Attorney General)*, [1999] 1 S.C.R. 743 at para 15. The phrase is interpreted broadly. The Court notes that "the natural and ordinary meaning of this phrase is that anything relevant or rationally connected to the incident under investigation, the parties involved, and their potential culpability falls within the scope of a warrant." In other words, the phrase in s. 487(1)(b) refers to any material that might shed light on the circumstances of the event that constitutes the offence.

[36] That said, a judicially authorized search must be conducted in a reasonable manner and must be no more intrusive than is necessary to achieve its objectives. As noted by Cromwell J. in *Vu*:

> [22] First, the police must obtain judicial authorization for the search *before* they conduct it, usually in the form of a search warrant. The prior authorization requirement ensures that, before a search is conducted, a judicial officer is satisfied that 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 the goals of law enforcement. Second, an authorized search must be conducted in a reasonable manner. This ensures that the search is no more intrusive than is reasonably necessary to achieve its objectives. In short, prior authorization *prevents* unjustified intrusions while the requirement that the search be conducted reasonably limits potential abuse of the authorization to search.

[37] Justice Cromwell went on in *Vu* to explain that searching electronic storage devices can be tricky and warned that the imposition of protocols that are too restrictive risks creating blind spots in an investigation. He said:

> [57] Second, requiring search protocols to be imposed as a general rule in advance of the search would likely add significant complexity and practical

> difficulty at the authorization stage. At that point, an authorizing justice is unlikely to be able to predict, in advance, the kinds of investigative techniques that police can and should employ in a given search or foresee the challenges that will present themselves once police begin their search. In particular, the ease with which individuals can hide documents on a computer will often make it difficult to predict where police will need to look to find the evidence they are searching for. For example, an authorizing justice's decision to limit a search for child pornography to image files may cause police to miss child pornography that is stored as a picture in a Word document. In short, attempts to impose search protocols during the authorization process risk creating blind spots in an investigation, undermining the legitimate goals of law enforcement that are recognized in the pre-authorization process. These problems are magnified by rapid and constant technological change.

[38] Mr. Fardy complains that the police scoured and/or rummaged around in his device for evidence beyond what the ITO would support. For example, aside from the fact that the warrant did not authorize a search of his internet history, there was absolutely nothing in the ITO referencing pictures, videos, or emails. The Crown says the ITO provided the issuing judge with enough evidence to allow inferences to be drawn to support a full search of Mr. Fardy's iPhone, except for the internet history.

Generalizations

[39] Mr. Fardy submits that the affiant's assertions about people being constantly connected to their phones, advanced in support of the authorization, if deemed judicially acceptable, would essentially allow the police to search anyone's phone, in any situation.

[40] The paragraphs of the ITO that he complains about in this regard are:

> a. Based on my experience as a police officer and my own personal experiences in communicating with my spouse, my friends, my colleagues and my family, that in society today, we are constantly connected to our phones and we are in constant communication with others;
>
> b. Mr. Fardy would have been in communication with the victims or with other people around the time of the offences via his cellular phone;

[41] The defence makes the following submission:

> Aside from the isolated messages mentioned by E.L.and S.M., there is nothing in the ITO to specifically suggest that Mr. Fardy's iPhone would contain evidence

> relevant to the allegations. There was no allegation that a device was used before, during or after the commission of any of the offences, or that Mr. Fardy made statements online or in messages that were relevant to the incidents. The July 30 messages that Mr. Fardy received from "Aaron" were plainly just words of encouragement from a friend arising from his arrest.
>
> In many cases device warrants have been upheld despite a lack of explicit evidence that the device was involved in the alleged offence, because a reasonable inference could be drawn based on other evidence or the integral role of communication in the offence (for instance, drug trafficking, human trafficking and conspiracies).
>
> The question is whether such an inference can also be drawn from the mere fact that everybody today is "constantly connected" such that it is now a likelihood, not merely a suspicion, that devices will contain evidence whenever an offence is alleged. Put simply, the premise of the ITO is that social media and messaging apps are bound to contain something relevant simply because devices are integral to our lives today.
>
> But this is the very concern addressed by ***R. v. Vu*** and ***R. v. Fearon*** almost a decade ago: the immense capacity of devices to continuously capture and store personal information calls for more careful prior judicial scrutiny; not less. It was for this reason that a lawful arrest, although necessarily based on reasonable grounds, was considered to be insufficient justification for a thorough search of the accused's device and the consequent risk of "wholesale invasion of privacy" (***R. v. Frearon*** at para. 58).
>
> The police request to search for data created 90 days after the date of the final allegation clearly demonstrates their intention to rummage around in the hope of finding something incriminatory. The ITO does not even remotely explain how or why evidence relevant to the allegations would have been generated in that period. Furthermore, police were aware that the allegations had begun to surface publicly and Mr. Fardy would likely have been seeking advice and preparing to respond to them, yet no protocol was put in place to prevent a possible breach of his solicitor/client privilege.
>
> Once police had the warrant, they searched the device indiscriminately. No effort was made to restrict the search based on nature of the data, parties to communications, geolocation, etc.
>
> If the search of Mr. Fardy's device is *Charter* compliant, it is very difficult to imagine what could possibly restrain the police in any other case. They may already be pre-printing ITOs with just one paragraph explaining that we're all constantly connected. [Emphasis added]

[42] In *Morelli*, Fish J., for the majority, considered generalizations about an offender's *propensity* made by the police in an ITO. He said:

[78] These people all commit child pornography offences, but the "propensities" of one type may well differ widely from the "propensities" of others. There is no reason to believe, on the basis of the information in the ITO, that *all* child pornography offenders engage in hoarding, storing, sorting, and categorizing activity. And there is nothing in the ITO that indicates which specific subset of these offenders does generally engage in those activities.

[79] To permit reliance on broad generalizations about loosely defined classes of people is to invite dependence on stereotypes and prejudices in lieu of evidence. I am thus unable to agree with Justice Deschamps (at para. 162) that the ITO's claims in this regard could properly be relied on by the justice.

…

[81] That some child pornography offenders do seek out and hoard illegal images is, of course, neither surprising nor helpful in determining whether reasonable and probable grounds exist in a particular case. Still, it is not the role of courts to establish by judicial fiat broad generalizations regarding the "proclivities" of certain "types" of people, including offenders. Matters of this sort are best left to be established by the Crown, according to the relevant standard — in this case, reasonable and probable grounds for belief. As suggested earlier, moreover, courts must be particularly wary of endorsing such generalizations when, as in this case, the crime alleged is the subject of intense emotional responses and widespread condemnation, and the temptation to rely on stereotype rather that evidence is therefore especially dangerous and strong.

…

[90] While it may be true that the accused was adept at recording videotapes and storing the tapes for future use — as is nearly everyone who owns a camcorder — this says absolutely nothing about his propensity to store a completely different kind of image (child pornography), in a completely different medium (a computer, as opposed to videotape), acquired in a completely different manner (downloading, as opposed to filming).

[91] The mere fact that a person collects, reproduces, or stores *anything* — music files, letters, stamps, and so forth — hardly supports an inference that he or she is of the type to hoard illegal images. To draw that inference here is to speculate impermissibly. At its highest, the proposed inference might provoke suspicion in some. And, as a matter of law, suspicion is no substitute for reasonable and probable grounds to believe either that the appellant committed the alleged offence or that evidence of the offence would be found in his computer.

…

[95] In short, as mentioned at the outset, the ITO in this case is reduced by scrutiny to two links in the browser's list of "Favourites" — links that were known to have been erased four months earlier. At best, this may be a ground for suspicion, but surely the deleted links afford no reasonable and probable grounds

> to believe that the appellant was in possession of child pornography, and still less that evidence of that crime would be found upon a search of his computer. [Emphasis added]

[43] Broad generalizations about categories of offenders without evidence to connect those generalizations to the specific accused do not allow for a reasonable inference to be drawn. However, is the ubiquitous use of mobile phones to communicate, whether orally or by text, really a broad generalization comparable to the alleged hoarding of images by pedophiles? In this case the Crown says that there are specific facts which allowed the issuing justice to draw the requisite inference.

Ubiquitous use of mobile devices

[44] Connected to the generalizations of an offender in this case, is the notion of ubiquitous use of mobile phones. In *Abo Zead*, Sharma J. discussed the search and seizure of mobile phones based on common knowledge of their widespread use, and reviewed the earlier decision in *R. v. Ferguson*, 2018 BCSC 490:

> [46] The ITO, the relevant portions of which are summarized at paras. 29–36, did not disclose any observations of the accused or his associates using cell phones. Indeed, the paragraphs in the ITO that conveyed the affiant's belief that a forensic examination of data from the phones would assist in the investigations did "not provide any details or specifics on how, or in what way, the seizing officers thought 'forensic examination and recovery' would assist" (at para. 34).
>
> [47] In support of the ITO, the Crown in that case stated that it was a "notorious fact that people today – especially young people – communicate extensively with mobile devices" and that they "take photos and videos using mobile devices" (at para. 60). The Crown noted that this material, if found on a device, could provide direct evidence of offences. The Crown went on to argue "that in light of this common sense reality, the authorizing justice was entitled to put 'two and two together'" from the facts set out in the ITO and make reasonable inferences that were not specifically articulated by the affiant (at para. 61). These inferences included that the three men had been staying together for months, and so were associated with one another, and that they were in joint possession of the firearms.
>
> [48] Justice DeWitt-Van Oosten agreed with the Crown and found that the ITO set out sufficient facts for the authorizing justice to make a number of necessary conclusions, which are listed at para. 74. Specifically, the court concluded that the relationship between the three men, particularly that they travelled to Vancouver together and had been staying together, was a reasonable basis upon which the authorizing justice could infer that they would have communicated during that

time frame with mobile devices found in their possession (para. 75). The warrant was upheld.

[49] As part of her reasoning, DeWitt-Van Oosten J. relied on the following observation that the police are not obliged to establish with certainty that the requested search will produce direct evidence of the offence in question:

> [67] Moreover, as explained in *CanadianOxy Chemicals Ltd. v. Canada*, I am to remain cognizant of the fact that s. 487(1) of the Criminal Code does not require of police that they show the search will produce direct evidence of the offences named in the warrant.
>
> [68] Rather, s. 487(1) has been broadly construed and authorizes police to "locate, examine and preserve all the evidence relevant to events which may have given rise to criminal liability" for the named offences: *CanadianOxy Chemicals Ltd. v. Canada* at para. 22….

…

[53] The applicant acknowledges the ITO could be seen as outlining reasonable grounds to believe the applicant and F.J. were involved in suspicious activity linked to the physical supply of firearms to Mr. Samra. However, he submits the ITO does not disclose a single investigatory observation suggesting the applicant used his phone in connection with any alleged suspicious activity. On that basis, he submits the ITO is deficient.

…

[55] The Crown submits the absence of observations of the applicant using a cellphone is not fatal to the Samsung Warrant, pointing out that no such observation grounded the warrants upheld in *Ferguson*. It was sufficient that there were enough facts establishing an association among the individuals sufficient to infer they may have been involved in a joint criminal enterprise. Combined with the ubiquitous use of cellphones, the court was satisfied a reasonable basis existed for searching the phones.

[56] The Crown points out the ITO does contain observations of F.J. using his cellphone. Once during undercover operations in scenario 33. Specifically, surveillance video captured images of F.J. being on his phone on two occasions contemporaneous with his stealing back the firearms. Also, as noted above, he attempted to use his phone to make or answer a call during his arrest.

[57] The applicant submits that at best, the preceding observations amount only to a suspicion, rather than a reasonable inference, that F.J. made calls connected with the alleged firearms trafficking. He asserts little can be assumed about the purpose, topic, or recipient of the calls observed.

[58] I disagree. The law does not require an inference to be the only explanation of events observed for it to be reasonable; nor is it necessary to rule out innocent explanations of observations. Given the observations that F.J. contemporaneously used his phone as the guns (which he had been involved in putting in the covert

> vehicle) were stolen back, it would, with respect, defy common sense not to conclude such an inference was reasonable.
>
> …
>
> [62] In my view, viewed all together, the preceding provides credibly-based and reasonable grounds to support both warrants, notwithstanding the absence of observations recorded in the ITO of the applicant using his phone.
>
> …
>
> [95] The Crown further submits that even if the affiant had not explicitly expressed a belief that the applicant and F.J. would send and receive photographs, it is a logical inference that could be drawn, therefore open to this Court to consider. In *Ferguson*, the court held the failure to articulate an inference is not fatal (at para. 106). In that case, the ITO similarly did not explicitly mention possible multimedia. Justice DeWitt-Van Oosten concluded the issuing justice could have drawn that inference and specifically referred to the likelihood firearms were obtained from others as a basis for this conclusion (at para. 86). I find Crown's position is sound. [Emphasis added]

[45] As noted by Sharma J. in *Abo Zead*, in *Ferguson*, Dewitt-Van Oosten J. considered the ubiquitous use of mobile phones. She said:

> [60] Moreover, it is a "notorious fact that people today – especially young people – communicate extensively with mobile devices" and that they "take photos and videos using mobile devices". This sort of material, if located on the devices, "could show communications, or associations, or photographs, or video, that provided direct evidence of the offences, or that provided evidence "respecting the commission" of the offences".
>
> …
>
> [75] In addition to drawing these conclusions (or inferences), I agree with the Crown that given the relationship between Witness X, Gino McCall and the accused, including the fact that they knew each other from Hamilton, two of them travelled to Vancouver together, and all three had been staying at City Centre, with at least two of them in the same room, it was also reasonably open to the authorizing justice to infer that the three men would have been communicating with each other during this timeframe, including through the use of mobile devices found in their possession, direct or constructive.
>
> [76] Between the F350 and room 127, police located six mobile devices. At least one of the devices was positively shown to be "active"; two of them were with the detainees as they travelled in the F350; and one of the devices located in room 127 had a British Columbia Area Code assigned to it (604), from which the

authorizing justice could infer that steps had been taken to activate this phone post-arrival from Ontario.

[77] In *R. v. Riley*, [2009] O.J. No. 738 (Ont. Sup. Ct.) at para. 134, Dambrot J. opined it is "no great leap in logic to conclude that a man who commits a murder in concert with others to further the interests of a gang that is engaged in a gang war, will discuss the murder, however covertly, with his confederates".

[78] In *R. v. Pangman,* 2000 MBQB 85 (CanLII), [2000] 8 W.W.R. 536 (Man. Q.B.) at para. 34 [cited in *R. v. Riley*], Krindle J. made a similar observation: "It is a reasonable inference that persons who are known to one another and who trust one another are likely to speak to one another about areas of mutual interest and concern".

…

[82] In reaching this determination, I have reminded myself that an inference is a "deduction of fact that may logically and reasonably be drawn from another fact or group of facts found or otherwise established by evidence adduced at trial … [Moreover, a] single item or several items of evidence may give rise to more than one inference …": *R. v. Tsekouras,* 2017 ONCA 290 at para. 229, leave to appeal ref'd, 2018 CarswellOnt 2055 (S.C.C.).

…

[85] Text messages and emails housed on the mobile devices would also logically afford evidence against which police could test the "defences" asserted by the detainees in their statements. For example, both Gino McCall and the accused denied knowledge of the fact that the F350 was stolen. All three men denied knowledge of the firearms, although two of them acknowledged seeing the suitcase at City Centre in the days prior to June 14.

…

[104] In that case, police obtained a warrant authorizing a residential search, including a search for documents that would identify the owners or occupants of the residence: at para. 4. At trial, it was conceded on the s. 8 *voir dire* that the ITO in support of the warrant "contained no statement concerning [the affiant's] grounds to believe that documents evidencing ownership or occupation would be found in the residence": at para. 14. [Emphasis added.]

[105] However, this did not preclude the Supreme Court from finding that a warrant for a search of documents in the residence could issue:

> [16] The question for the reviewing judge 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 … In applying this test, the reviewing judge must take into account that authorizing justices may draw reasonable inferences

> from the evidence in the ITO; the informant need not underline the obvious …
>
> [17] The ITO set out facts sufficient to allow the authorizing justice to reasonably draw the inference that there were reasonable grounds to believe that documents evidencing ownership or occupation would be found in the residence: A.R., vol. II, at p. 112. In particular, the ITO referred to the premises to be searched as a "residence" and as a "two (2) story house" (p. 111). It also indicated that the appellant owned the property and that electricity was being consumed there: pp. 110-11. In my view, it is a reasonable inference that a residence would be the place to look for documents evidencing ownership or occupation. Where else would one expect to find such documents if not in the residence itself? Moreover, I think that the authorizing justice could reasonably infer that a place was being occupied as a residence from the fact that electricity was being consumed at that place and that it had an owner.
>
> [18] I therefore conclude that the authorizing justice could lawfully issue the warrant to search for documents evidencing ownership or occupation of the property.

[106] As made manifest in these highlighted passages, inadequately articulated grounds to believe (or even an absence of articulated grounds), is not fatal to the issuance of a warrant if the facts laid out in the ITO allow the authorizing justice to reasonably draw an inference that grounds exist. I have found, in this case, that it was reasonably open to the authorizing justice to do so. See also *R. v. Ali-Maliki* at para. 14: "Sufficiency … does not require flawlessness". [Emphasis added]

[46] Similarly, in *R. v. Belcourt*, 2012 BCSC 796, Macaulay J. stated:

> [9] Text messaging is a common, if not ubiquitous, means of communication between young people in particular. It is likely the least expensive form of cellular phone communication available and not surprisingly, the accused in this case used it extensively. A review of the text messages produced as a result of the production orders reveals many personal and intimate communications with their girlfriends. The review also reveals that texting was a means to communicate about criminal activities.

[47] The Crown has therefore put forward authority for the proposition that: 1) the use of texting and electronic communication between young people is ubiquitous and; 2) when interaction between an accused and others occurs where communication about the crime might be expected, an issuing justice can properly draw an inference that the use of mobile phones may have taken place, and searching the accused's mobile phone may afford evidence.

Persons involved in criminal enterprises speaking to each other

[48] The Crown relies on several cases where the inference has been considered proper that, as noted above, persons involved in criminal enterprises will communicate with each other. Here we have only one accused, but he is alleged to have committed crimes in social situations where communication with the complainants might be expected. Additionally, as a result of text messages that were sent to his phone at the same time as he was being arrested, he is alleged to have communicated with his friends via text about the alleged crimes. Specifically, the Crown points to the text message allegedly sent by Mr. Fardy to E.L. asking her out; the text message sent by S.M. to Mr. Fardy asking him what had happened the night before, and his alleged text reply that "I was too high and horny"; Mr. Fardy's texts to and calls with J.M.'s ex-boyfriend, T.O., harassing him and/or asking him to fight on the night of the alleged sexual assault on J.M.; and the texts observed by the police being sent to Mr. Fardy's phone from "Aaron" stating "innocent until proven guilty", "don't say a fucking word" and "we're gonna get you through this". The Crown says these messages provide a credibly-based probability that Mr. Fardy's phone will afford evidence relevant to the offences.

[49] With regard to the communications between Mr. Fardy and his friends, the Crown points to *R. v. Pangman*, 2000 MBQB 85, where Krindle J. stated:

> [34] It is a reasonable inference that persons who are known to one another and who trust one another are likely to speak to one another about areas of mutual interest and concern. It is a reasonable inference that individuals finding themselves arrested and charged with the types and numbers of offences that these accused were charged with are likely to be concerned about what has just happened to them. It is a reasonable inference that learning that a formerly trusted, high-ranking member of the organization was now co-operating with the police about the activities of the organization and its members is likely to be of concern to those connected to the organization. It is a reasonable inference that such affected individuals are likely to talk about their common areas of concern. The very argument used by the defence itself to allege state manipulation of the accused in the previous section of this judgment – namely, that if they are put together, of course they are going to talk, notwithstanding their expressed choice not to speak to the state – serves to underpin just how very reasonable was the inference drawn by Hewak C.J.Q.B. In addition, it is a reasonable inference that observation of the dynamics of the interaction amongst 35 people connected to a structured organization and holding different positions

> within that structure is likely to provide evidence of that structure, regardless of the specific topic of discussion amongst them. [Emphasis added]

[50] Similarly, in *R. v. Riley*, 2009 CanLii 7177 (ONSC), Dambrot J. discussed the basis on which an authorizing judge could have found that evidence of a murder in a gang war context would be obtained by intercepting private communications:

> [134] It is no great leap in logic to conclude that a man who commits a murder in concert with others to further the interests of a gang that is engaged in a gang war, will discuss the murder, however covertly, with his confederates. Added to this is the information contained in the affidavit that the members of the gang tended to congregate at Maxeen McPherson's residence where they hung out after their shootings, watched the news in order to ascertain what the police knew, and discussed what they heard. They also hung out at the Head to Toe Beauty Salon and Dana Williams' residence. Finally, the fact that Riley and Atkins had been arrested in connection with another gang-related shooting was likely to stimulate discussions about their jeopardy for that and other of their crimes. In all of these circumstances, there was a high probability that intercepting their discussions at McPherson's residence, the beauty salon, Williams' residence and elsewhere would assist the investigation into the murder of Charlton, and provide evidence of that offence. The authorizing judge was certainly entitled to reach that conclusion.

[51] That Mr. Fardy communicated electronically with his friends about the allegations was one logical inference available to the issuing justice, and even if the communications were in relation to possible defences, according to *CanadianOxy Chemicals Ltd. v. Canada (Attorney General)*, that inference would support the issuing of the search warrant.

Overbroad search and seizure

[52] Mr. Fardy says the search of his phone was conducted in an overbroad manner. In *R. v. Barwis*, 2022 ABQB 561, Labrenz J. thoroughly reviewed the issue of an overbroad search and stated:

> [89] I accept that I have a responsibility to minimize a search that would otherwise be unreasonably expansive and in violation of an individual's right to be free from unreasonable search or seizure as protected by s.8 of the *Charter*. As noted by Moreau J (as she then was) in ***Marek***, relying upon Cory J's comments at para 49 in ***R v Nova Scotia Pharmaceutical Society,*** 1992 CanLII 72 (SCC),

[1992] 2 SCR 606, an analysis of overbreadth considers the means chosen by the state in relation to its purpose. The state must reasonably justify the necessity of its actions as measured by the objectives of the criminal investigation. The state's interest in investigating must always consider and concern itself with the privacy interests of individuals. The state must impair those interests as little as possible.

[90] An example of overbreadth is found in ***R v Rogers Communications,*** 2016 ONSC 70. In the factual circumstances considered there, involving the investigation of several jewelry store robberies, the police sought and obtained production orders for all cellphone records for phones activated, transmitting, and receiving data through all of Telus' towers proximate to 21 municipal addresses and 16 Rogers' towers. Telus estimated that this would result in the disclosure of the personal information of at least 9,000 customers and Rogers estimated that they would be disclosing information regarding 34,000 subscribers. After finding a s.8 *Charter* breach, Sproat J at para 65, provided valuable advice and guidance to ensure that future production orders would be minimally impairing.

…

[119] As Cromwell J stated in ***Vu***, there is generally no requirement for advance search protocols for computer searches. As Justice Cromwell further explains at paras 55-57, the manner of search is reviewed after the fact. In addition, the imposition of protocols would add significant complexity and practical difficulty and may actually "risk creating blind spots in an investigation" because it is difficult to predict in advance where relevant files might be found on a computer.

[120] At the same time, Justice Cromwell's comments cannot be taken to mean that the police are permitted to indiscriminately explore every bit of data in the hopes that it may uncover even the smallest trace of evidence. This is particularly true where, as here, the police are limited temporally in relation to what data may be searched. A relevant example is found in the circumstances of ***Marek,*** where Moreau J considered a search warrant relating to publication of obscene material on a website involving the murder and dismemberment of a human victim, Moreau J found a s.8 *Charter* breach because the police search of the accused's computer was conducted in a manner so as to export thousands of deleted emails, photos, videos and an entire Internet history that had no apparent relevance to the investigation. Justice Moreau stated at para 146 as follows:

> The effect of the search of Mr. Marek's personal computers was to export thousands of
>
> deleted emails, photos, videos, and an entire Internet history which had no apparent relevance to the investigation. While a cursory search of all files in a computer was found to be justified in ***Jones*** [2011 ONCA 632], exporting this material for the use of investigators and eventually the Court without applying a temporal filter, a technology available to Cst. Gainor at the time of the search, went well beyond the purposes of the

> investigation as set out in the ITOs. Crown counsel submitted that the best evidence as to ownership and control could arguably come from the genesis of the Website. However, there was no evidence in any of the ITOs suggesting that the Website was first registered in the early 2000's. There was, however, information relating to its registration as of 2012.
>
> …
>
> [125] In the present circumstances, however, the search of the accused's electronics conducted by Det. Neufeld in his home violated the accused's s.8 *Charter* rights. This is because the state's search must be conducted in a manner that respects the promises made to the authorizing judge within the ITO.

[53] To the extent that the search captured the internet history, it was conducted in an overbroad manner. The Crown does not propose to rely on that evidence, as noted earlier.

Failure to keep detailed notes

[54] Constable Marshall did not keep detailed notes while he was reviewing the electronic information retrieved from Mr. Fardy's phone. In particular, he did not keep clear notes of his search of the web history, for which there was no judicial authorization to search in the first place. Mr. Fardy submits that this is another constitutional violation.

[55] In *R. v. Villaroman*, 2018 ABCA 220, the majority stated, in relation to a police failure to take detailed notes:

> [17] Nor can we conclude that any failure to take detailed notes of the manner in which the search was conducted constitutes a section 8 breach in these circumstances. The appellant relies on guidance about the importance of note-taking which the Supreme Court provided in *Vu* and *R v Fearon*, 2014 SCC 77, [2014] 3 SCR 621. In *Vu*, Cromwell J noted that the officer's failure to take notes was "disquieting" and directed that "notes of how a search is conducted should […] be kept, absent unusual or exigent circumstances". <u>But he also noted this requirement was not a "constitutional prerequisite": para 70. Later, in *Fearon*, Cromwell J elevated the requirement to take notes to a constitutional requirement in cases where a police officer searches an electronic device incident to arrest:</u> para 82. Note-taking became mandatory in *Fearon* because the common law power to search incident to arrest is an "extraordinary search power that requires neither a warrant nor reasonable and probable grounds." Accordingly, there is a heightened need for police to take detailed notes, allowing courts to engage in after-the-fact review to determine whether a search was lawful and conducted

> reasonably. Even when police obtain a warrant based on reasonable and probable grounds, there may be some cases where the failure to take notes of a computer search could give rise to an inference that the police conducted the search unreasonably. On this record, however, we cannot draw such an inference. The forensic examiner testified at length about how he conducted the search. The failure to take detailed notes does not appear to have undermined the appellant's ability to meaningfully challenge the reasonableness of the search.
>
> [Emphasis added]

[56] Unlike the search of an electronic device incident to arrest, there is no constitutional requirement that the police take detailed notes when searching an electronic device as the result of seizure under the authority of a search warrant. However, detailed note-taking is urged by the Supreme Court of Canada, and, depending on the circumstances, the failure to keep detailed notes might support the argument that a search of an electronic device under a warrant was unconstitutional. In this case, Constable Marshall testified that he did not keep detailed notes. However, the only evidence to which this omission is relevant is Mr. Fardy's internet history, and the Crown is not relying on that.

Analysis

[57] I believe that it is reasonable to infer that people, including persons in their late teens and twenties (as is the age range here), use mobile devices to communicate ubiquitously, including the use of messaging apps. However, in order to search a mobile device, there must be more than that inference. And there was much more in this case. The ITO indicated that multiple complainants gave detailed statements alleging that Mr. Fardy sexually assaulted and assaulted them. Mr. Fardy was charged with multiple counts of sexual assault and assault in relation to five complainants over a four-year span. According to the ITO, he "was either acquaintances of or dating" the complainants in and around the time of the alleged crimes. He is alleged to have used his phone to ask out one of the complainants via text; to briefly discuss the allegations via text with a separate complainant; to harass the ex-boyfriend of another complainant and/or asked him to fight via text on the night of an alleged offence; and to receive text messages at the time of his arrest that imply that he had discussed the offences with his friend.

[58] There is clearly a credibly-based probability that Mr. Fardy's iPhone would afford evidence relevant to the investigation, in particular text messages, or texting

through apps such as Snapchat or iMessage, in relation to communications with E.L., S.M. and T.O. Similarly, the texts from "Aaron", could reasonably be inferred to be Mr. Fardy's friend, Aaron Cameron, and one available inference is that Mr. Fardy discussed the allegations with him. All of those communications achieve credibly-based probability on these facts

[59] In relation to the communications with the other complainants, as well as the authorization to search and seize communications with the other complainants, the relationship between Mr. Fardy and those complainants and the allegations were such that, considering Mr. Fardy's use of his phone with E.L. and S.M., one inference available to the issuing justice was that Mr. Fardy and those other complainants communicated in a similar fashion. As such, there was a credibly-based probability that the messaging apps in Mr. Fardy's phone would afford evidence relevant to the investigation.

[60] Despite the strong warnings from the Supreme Court of Canada against the police scouring computers and mobile phones for evidence, if there is a credibly-based probability that the device will afford evidence relevant to the investigation, then there is no constitutional violation. Therefore, I must consider whether one such inference was available to the issuing justice in relation to the pictures, videos and emails stored on Mr. Fardy's iPhone. According to the ITO, Mr. Fardy was either in a relationship with each of the complainants, or knew them in some way, prior to the alleged sexual assaults. The ITO goes on to claim that he sexually assaulted the complainants, acted subsequently as if his interactions with them were reasonable, and communicated by text with two of them. One of the possible apps allegedly used between S.M. and Mr. Fardy, Snapchat, generally involves the sharing of pictures when sending a text. Nothing else in the ITO, however, referred to the use of Snapchat by Mr. Fardy. As noted above, I agree that use of mobile phones is ubiquitous. Historically, prior to the advent of mobile phones, so was the use of landline telephones and Parliament legislated very specific wiretap legislation to deal with listening to those conversations. As the Supreme Court of Canada has stated, the information stored in mobile phones and personal computers is more private and personal than anything else in human history.

[61] This situation is not analogous to the cases involving gangs or criminal conspiracies, where the police affiant does not have access to first-hand knowledge of communications between the accused and other relevant persons, and therefore the issuing justice has to draw more strained inferences regarding modes of communication. Nor is this analogous to the possibility that a child pornographer

will try to hide images in other types of files. In this case, the ITO contained detailed summaries of the complainants' evidence, and those summaries did not reference emails between Mr. Fardy and anyone else, nor was there reference to photos or videos. Some of the complainants alleged that they were impaired or unconscious when Mr. Fardy sexually assaulted them. Of course, it is possible to suspect that a sex offender might take photos or videos of the complainant or the sexual activity in those situations, but this hunch would be akin to the "inference" that all pedophiles hoard images. As noted in *Morelli*, this would not be a *reasonable* inference supported by the evidence, but would be one based on improper propensity reasoning.

[62] Even considering the high standard of deference I must show to the issuing justice's decision, considering the strong warnings from the Supreme Court of Canada regarding the elevated expectation of privacy in a mobile device, I do not think that a reasonable inference was available to the issuing justice to permit the search of Mr. Fardy's emails, photos and videos. I agree that the search of his phone for photos, videos, and emails equated to scouring or rummaging through his phone looking for evidence on a hunch or mere suspicion. Mr. Fardy's s. 8 *Charter* right were violated in that regard.

[63] In this case, the failure of the police to keep detailed notes while searching the phone under the authority of a warrant was not constitutionally required and on these facts is not a s. 8 *Charter* violation.

Conclusion

[64] The ITO supported the inference that there were reasonable grounds to believe that Mr. Fardy's Apple iPhone would afford evidence of 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, and/or would afford evidence with respect to the commission of an offence.

[65] The ITO supported the issuance of a warrant allowing the search of Mr. Fardy's phone for messages (SMS, MMS, etc.); call logs; and social media application messages (Facebook, Instagram, etc.) between Mr. Fardy and the complainants, Mr. Fardy and related witnesses, as well as Mr. Fardy and his friends. The search and seizure of those items did not violate s. 8 of the *Charter*. There is no constitutional violation regarding that evidence.

[66] However, on the basis of the facts presented in the ITO, no reasonable inference was available to the issuing justice allowing a search of Mr. Fardy's phone for photos, videos or emails, and as conceded by the Crown, Mr. Fardy's internet history. Therefore, those items were seized in violation of s. 8 of the *Charter*.

[67] The parties asked to have a separate hearing regarding a remedy under s. 24(2) of the *Charter*, once my decision was rendered regarding s. 8 of the *Charter*.

Arnold, J.