
CANADA / JUDGMENT

R. v. Caza

2012 BCSC 525

COURT

Supreme Court of British Columbia

DECIDED

11 April 2012

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

2012 BCSC 525 R. v. Caza

IN THE SUPREME COURT OF BRITISH COLUMBIA

Citation:

R. v. Caza,

2012 BCSC 525

Date: 20120411

Docket: 89263

Registry: Kamloops

Regina

v.

David James Caza

Before: The Honourable Mr. Justice Powers

Ruling Re: Voir Dire #1 - Search & Seizure

Counsel for the Crown:

B.P. Caffaro

Counsel for the Accused:

J.P. Gustafson

Place and Date of Trial:

Kamloops, B.C.

February 13 -17, 20, 21, 23, 24, 27 - 29, March 1, 2, 5 - 9, 12 - 16, 19 - 22, 26 - 29, April 2 & 3, 2012
(and continuing)

Place and Date of Decision:

Kamloops, B.C.

April 11, 2012

Place and Date of Judgment:

Kamloops, B.C.

April 11, 2012

Introduction

- [1] The RCMP attended at Mr. Caza's residence on January 13, 2010. Mr. Caza was arrested and told he was being charged with possession of child pornography and possession with the intent to distribute and breach of a court order. The police had a search warrant for the search of his residence. Mr. Caza was taken into custody and his apartment was searched that afternoon. Subsequently, the RCMP realized that some items had been left in the apartment that should have been seized. They obtained a second search warrant and attended the apartment on January 20, 2010 and completed a second search and seizure.
- [2] Mr. Caza seeks to have everything seized by the RCMP on either search excluded as evidence in the trial. He argues that the searches were unreasonable and in breach of his rights under the Charter of Rights and Freedoms, (the "Charter") s. 8, which provides:
8. Everyone has the right to be secure against unreasonable search or seizure.
- [3] The searches were conducted pursuant to a search warrant but Mr. Caza argues that some of the information on which the search warrant was based was itself obtained by an unlawful search and should be excised from the information to obtain. He argues that when all of that evidence is excluded from the information to obtain that there is insufficient evidence left to support the warrant. Therefore he argues that the warrant should not have been issued and that the search in essence was a warrantless search. He initially argued that some of the information to obtain was misleading and that should also be excluded. He is no longer taking that position.
- [4] He applies for an order that the evidence should be excluded pursuant to s. 24(2) of the Charter:
- (2) Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.

The Law

- [5] In the recent decision *R. v. Wilson*, 2011 BCCA 252, Mr. Justice Frankel, writing for the court said the following:

37 The test to be applied in determining whether a search warrant (or wiretap authorization) was properly issued is well-known. It is often referred to as the Garofoli test, as it was first articulated by the Supreme Court of Canada in *R. v. Garofoli*, [1990] 2 S.C.R. 1421 at 1452. That test has been affirmed and applied by that Court in a number of cases: e.g., *R. v. Bisson*, [1994] 3 S.C.R. 1097; *R. v. Pires*; *R. v. Lising*, 2005 SCC 66, [2005] 3 S.C.R. 343 at para. 30; *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253 at para. 40. Recently, in *R. v. Bacon*, 2010 BCCA 135, 285 B.C.A.C. 108 at para. 25, leave to appeal ref'd [2010] S.C.C.A. No. 213, Mr. Justice Donald adopted the following as a succinct statement of that test:

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. While evidence of fraud, material non-disclosure, or misleading information are all relevant to this enquiry, their sole impact is to determine whether there is a continuing basis to support the warrant: ...

Defence Position

- [6] When the voir dire opened Mr. Gustafson indicted that in regard to the search his position is that the initial investigating police detective gained access to the computer of a person in the US. Using that person's computer password he was able to log on to a peer-to-peer site known as "GigaTribe". The US person had a number of contacts including one referred to as "Paper123boy". Mr. Gustafson argues that by using the US password and GigaTribe account the detective was able to look into the computer in which the Paper123boy information was stored and see some of the contents. He argues that this amounted to a warrantless search. He argues that Paper123boy had an expectation of privacy and because of the special nature of this peer-to-peer group only those people who were contacts could see that information. He does not admit that the accused is Paper123boy, but says the hard drive searched was connected to the accused's computer and therefore an unreasonable search of the accused's computer.
- [7] He uses the analogy that this is like a perimeter search of a residence where the police conduct an unwarranted and unlawful search to obtain information and then rely on that information to obtain a warrant. He also argues it was like giving a friend a key to your house. If the police arrest that person, they are not entitled to use the key to come into your house to see if they can obtain information to support a search warrant.
- [8] He also argues that when the police downloaded some of the information that was being offered by Paper123boy to the US user that they used what was called a "packet sniffer" to obtain the IP address that accompanied that information. They were then able to use the IP address to find that this was connected to a Shaw Communications Inc. ("Shaw") account in Kamloops.

- [9] He argues that when the police then requested the name and address of the account-holder that had been using that IP address on that particular day that this again amounted to an unlawful search.
- [10] He argues that without this information they would never have connected anything on the computer to the residence at 110 Columbia Street, Apartment # 34.
- [11] Therefore, he argues that all of this amounted to what was really a warrantless search and that the results of that search should be excluded particularly because the search involved a place where a person had a high expectation of privacy, that is their residence and their computer.

Background

- [12] The investigation which led to the arrest of Mr. Caza and the search of his apartment began with the efforts of Detective Paul Krawczyk, a member of the Toronto police force. He is an expert in computer forensics and has expertise in detecting and investigating non-electronic and electronically-generated child pornography. He is an expert on the patterns and methods of personal use and distribution of child pornography, particularly with regard to computers and the internet. He has expertise in the organization of child pornography collections and the use of equipment and computer techniques by collectors of child pornography. He also has expertise in the way in which child pornographers, collectors or pedophiles operate.
- [13] He also has expertise in a particular peer-to-peer internet site known as GigaTribe. Detective Krawczyk advised that this particular peer-to-peer website is different from the norm. In most peer-to-peer websites anybody that is a user or member of that website can see postings and obtain material from any of the other members. In this particular website however, when you become a user you may be able to see the public profile of other users but you can only share or transfer information with people who have accepted you as a contact or who you accept as a contact. Users may employ different methods to determine who they will accept as contacts. Users may accept anybody or they may require a recommendation or verification from some user they are already familiar with before they accept a new user. Users can delete people from their contact list at any time. If you have a user account, and your GigaTribe account is open, then any of the users on your contact list, using their account, can see the things that you are offering to share. The things you are offering to share may appear as thumbnails and the other contacts can simply click on that item to see what it is and then download it if they wish. You do not have to be at your computer to allow this to occur. You do not have to do anything other than offer to share. The contacts can only see what you are offering to show them and they do not have general access to your computer. They only have access to those items which you are offering to share.

- [14] You may send messages to your contacts either individually or as a group. If you send a contact a message it will remain available to that contact and be visible to them when they open their user account. They could then read that message on their account.
- [15] Once one of your contacts has accepted an item that you have offered to share they have a copy of it on their computer and can do with it as they please.
- [16] Users of this site do not have to provide any personal information including email accounts. They remain completely anonymous. Other users would only know them by their user name. The user account will have a name and password. However that does not mean that the user account is only being used by one person nor that it remains in the control of one particular individual. Nor is there any information as to who that individual might be, whether they are a person interested in child pornography or a police officer investigating child pornography. There is no information about whether this is a single individual or a group of individuals. There is no information available about when a user name or account changes hands or is being used by somebody different from the original user, or being shared by the user.
- [17] Detective Krawczyk's evidence is that this peer-to-peer website seems to be used only by people interested in sharing child pornography. The site appears to be updated from time to time to improve its usability. It has the ability to download very large files very quickly and easily. Detective Krawczyk's evidence was that many of the people using this site were collecting and sharing child pornography and go to a great deal of effort to organize and sort their material. This makes them more valuable as a trading partner.
- [18] When you decide to accept somebody's contact you have no control over what steps they may take to protect the security of their computer or any information you may choose to share with them. They require a password for their account but you have no control over what steps they take to secure that password.
- [19] Detective Krawczyk became aware of this peer-to-peer site and of a person who had a user account. Through communications on the website with that person he was able to determine the IP address for their computer. He was able to locate the account name and address associated with that IP address. The account name and address associated with the IP address was in Newfoundland. Detective Krawczyk provided the information he had to the Newfoundland constabulary who made the arrest. They seized that individual's computer and were able to obtain his password for his GigaTribe user account. They provided this information to Detective Krawczyk. Detective Krawczyk then used that person's user account and password to find that person's contacts. One of the contacts was a person in Tennessee, Dan Quail. His user name was "Devthedude2008". Detective Krawczyk was able to determine Quail's address and provided it to the United States Homeland Security Department who deal with internet child pornography crimes. They arrested Quail and seized his computer. They were able to obtain his password for his GigaTribe account and provided that information to Detective Krawczyk. Detective Krawczyk was able to access

Quail's GigaTribe account and find his list of contacts. One of the contacts was Paper123boy.

[20] On January 5, 2010, Detective Krawczyk opened Quail's GigaTribe account and found messages which had been stored, because they were received while the computer was disconnected. Those messages were all from Paper123boy for Devthedude2008. The messages began with the words "[Message received while disconnected] Paper123boy for Devthedue2008" followed by the date and time, they were as follows:

(12/29 19:57)

[USER775093:Paper123boy] (12/29 16:31): Littleboiz boys 5-13 looking for people that like to trade same

(12/30 12:01)

Reposting PICs folder picking the doubles out noticed it

(12/31 17:12)

Off for zzzzz seems other places are quiet at the moment

(12/31 17:13)

Oh no close to New years where A buddy is I can hang in another 15 min :)

(10/02 11:55)

<http://www.hotvideozone.com/broadcast/view/?id=3410210> live little boy sex show (at password) it may be 2 hours before they aply it though

(01/04 18:56)

New folder catrholic boys like smotri after these ones done playing in the snow will let them know more shows and so called porn kings the best guy there (used to be until it was taken from me) <http://www.hotvideozone.com/user/cartoonpa>

(01/04 18:58)

<http://www.hotvideozone.com/user/cartoonpaperboy/> would like them to do while sucking each others cocks and browsing SMOTRI SITES :):): please download so I can plan withte boys there is no smotri for me it was stolen by

(01/04 18:58)

assholes only onwe cared to here about I will be ioff for a while I rather play white bboys Smotri has disgusted me :):):)

(01/04 18:59)

those littel boys are 10 and 11 and know the interent very very well and ... at are smotri (but not broadcast) dont think any my friends here wil see the penis there

(01/04 19:20)

open folder schoolboyd smotri please download now I will be at boys house to show of Smotri maybe for some time

- [21] Detective Krawczyk did not access any computer or computer equipment attached to any computer that the accused may have had an interest in at this time. He was merely accessing Quail's GigaTribe account.
- [22] On January 6, 2010, Detective Krawczyk again accessed Quail's GigaTribe account and could see the messages and also saw that Paper123boy was offering to share some files. These were signified as thumbnails on the bottom of the page. Detective Krawczyk was able to click on those thumbnails and determine that they were child pornography. He clicked on those items and downloaded copies of them to his computer and in doing so was able to capture that information. He was also able to capture the IP address of the computer which was sending that information. He used a program he referred to as a packet sniffer to do this. That allowed him to capture copies of the material that was being downloaded as well as the IP address. Detective Krawczyk said that anybody with a standard Windows operating system can determine the IP address associated with any email or chat message that they receive or any other download they receive. The IP address is information that is attached to that type of message.
- [23] Detective Krawczyk was then able to use another website to find out which company owned that IP address. In this case it was Shaw. Detective Krawczyk sent an email request to Shaw to provide him with the account name and address of the Shaw customer that was using that IP address at the particular time. Detective Krawczyk referred to this as a law enforcement request. The police simply send a request to the internet service provider confirming that they are members of the police force and that they are investigating child pornography on the internet and seeking the specific user account that relates to a specific IP address at a specific time.
- [24] Shaw then provided the name of the person who had the account which was Brian Feltham and the address #34, 110 Columbia Street, Kamloops, BC. Detective Krawczyk forwarded this information to the British Columbia RCMP Internet Child Exploitation Squad. The information was then passed on to the Kamloops RCMP for the purposes of obtaining and executing a search warrant. The Kamloops RCMP were able to determine that Mr. Caza was the person who resided at the address associated with the account. They inquired of Mr. Caza's probation officer who at the time said they could find no connection between Mr. Caza and Brian Feltham. In fact, an earlier probation officer was aware that Mr. Feltham had resided with Mr. Caza briefly. The IP address and the information about the name and address of the account were essential information for the search warrant. This information allowed the police to make the connection between the child pornography being offered by Paper123boy and Mr. Caza's residence.

- [25] Mr. Caza was known to the RCMP and they prepared the information to obtain a search warrant of his residence.
- [26] Prior to this, Detective Krawczyk had done a Google search of the name Brian Feltham and did find a reference to him on an internet dating site. He had a user name of Brian123 and had last logged on in November of 2006. He was on a social network site and his user name was God Dude and his sexual preference was shown as heterosexual.
- [27] Detective Krawczyk said that in his experience the subscriber to an internet account may not necessarily be the user of that account. He conducted the Google search to try and determine who he might be dealing with in this investigation.
- [28] Detective Krawczyk was also concerned because in his initial investigation of Quail's user's account, some of the information from Paper123boy referred to Catholic school boys and photographs and what he interpreted to be live broadcasts. He was concerned that Paper123boy may actually be producing child pornography or be in contact with young boys. Some of the things offered for download included photographs which were taken with a Canon camera. These photographs still have the meta data attached to it which indicated they had been recently taken. The fact that the meta data was still attached to the photo images also indicated to him that they had probably been taken by Paper123boy. The photographs appeared to be of young children playing in a snow-covered school ground or playground. Detective Krawczyk then did a Google search of 110 Columbia Street in Kamloops, B.C. and determined that it was across the street from a school ground and close to two daycare centers and a youth center.
- [29] Constable Butler of the Kamloops RCMP was responsible for preparing the information to obtain the search warrants. She had received all of the information forwarded by Detective Krawczyk and additional information from the BC Integrated Child Exploitation Team. This included information about Mr. Caza, his address and the name of Brian Feltham. She also had copies of the material which had been downloaded from the Paper123boy user site. She knew the area of the residence and knew that there was a children's school across the street. She obtained a search warrant; that warrant was executed January 13, 2009. She attended at the residence and arrested Mr. Caza when he came to the door. She and a number of other officers conducted a search of Mr. Caza's very small apartment. They seized a Canon camera, a computer and an 80 gigabyte hard drive attached to that computer, and a large number of CDs and DVDs located in different locations in the apartment. They also seized a Motorola modem which was on the floor in the apartment and appeared to be connected to an internet cable in the wall and to the computer.
- [30] They seized a number of documents found in the apartment, some that appeared to relate to computer use and had what might have been emails of users' names on them. Some of the documents were accounts relating to a Shaw internet account. Some of the documents seized referred to Feltham and some referred to Caza.

- [31] The memory card from the camera was sent to the RCMP Forensic Unit in Ottawa to see what information could be retrieved from this card. Constable Butler and other members of the RCMP began checking the DVDs and CDs which they had seized. The computer and its hard drive were forwarded to an RCMP forensic expert in Vancouver for analysis. Approximately January 18 Constable Butler learned that although there was a GigaTribe account and some other software on the 80 gigabyte hard drive which was attached to the computer, there was nothing else. There was no child pornography and it appeared that this hard drive had not been used since November of 2009.
- [32] Constable Butler mentioned this in passing to Sergeant Mathieu who had assisted in the search. Sergeant Mathieu told her that he had found another hard drive and a cell-phone. This was the first that Constable Butler had heard of these items. She immediately obtained another search warrant in order to go back and retrieve these items as well as some VHS tapes which had been left behind. The warrant authorized them to seize the hard drive and the VHS tapes but not the cell-phone. She attended the apartment on January 20 and found a 500 gigabyte hard drive left on the end of a couch where Sergeant Mathieu told her he had left it. Sergeant Mathieu had a very vague recollection of exactly where he found this hard drive or where he left it. However he did remember finding it in the living room area and remembered a discussion about it although he thought the discussion occurred the day after the search or on the day of the initial search. The 500 gigabyte hard drive was also forwarded to the Vancouver forensic division for analysis.
- [33] One group of the DVDs or CDs found in one location were inspected by another member of the RCMP, itemized and catalogued. However those items went missing in the RCMP exhibit room in Kamloops, BC. The RCMP have been looking for them but have been unable to find them. I understand they are doing a complete audit of their exhibit room in Kamloops. Another group of DVDs and CDs have been available and marked as exhibits in the voir dire. Both hard drives and the computer tower have also been marked as exhibits in the voir dire. The modem connected to the internet in the computer has also been marked as an exhibit. The group of DVDs/CDs that was not lost was marked as an exhibit.
- [34] Through forensic analysis the RCMP have been able to determine that the 500 gigabyte hard drive was connected to the computer tower which was seized. The hard drive had been used just moments before the RCMP executed their search of the residence. It appeared that the hard drive had been disconnected "ungracefully". By that, Sergeant Collins who analyzed it meant that it was as if the power had suddenly been cut. The side of the computer tower was not on the computer tower and the computer was set up so it would be easy to connect or disconnect a hard drive. The 80 gigabyte hard drive which was physically connected to the computer when it was seized had not been activated since November of 2009. The 500 gigabyte hard drive had the external markings including serial numbers removed from it. However it does have an internal serial number which Sergeant Collins was able to obtain. The RCMP were able to confirm that hard drive had been purchased by a Mr. Caza from the Kamloops Computer Centre in Kamloops.

- [35] The 500 gigabyte hard drive had thousands of child pornographic images and videos and many chat messages. A number of the chats had been wiped clean but were still residing on the hard drive and were recoverable. The 500 gigabyte hard drive also had images that appeared to have been taken from the Canon camera seized in Mr. Caza's apartment. Some of the images from the camera looking out of the window of the apartment show a computer screen that appears to have the GigaTribe website on the screen. The child pornography images found on the DVDs and CDs are also on the computer hard drive.
- [36] Detective Krawczyk and Sergeant Collins both indicated that the material on the 500 gigabyte hard drive was very thoroughly organized and it appeared that the user had put in a great deal of time and trouble in order to arrange it.
- [37] This information is obviously vital to the Crown's case against Mr. Caza.

Defence Position

- [38] The accused argues that a person has a high expectation of privacy in their residence and in personal computers. (*R. v. Morelli*, [2010] 1 S.C.R. 253.) In *Morelli*, the Supreme Court of Canada recognized that a personal computer could be expected to contain all kinds of personal information, which the user would not want anybody else to see. At the minimum, that the user would want to restrict whoever else might see the contents of their computer.
- [39] The accused also argues that internet subscriber information, that is the name of an account holder and the address that attaches to that account, contains personal biographical information in which a person also has a high expectation of privacy. (*R. v. Cuttell*, [2009] O.J. No. 4053.) In *Cuttell*, the court had no information about the contract between the individual and the internet service provider, but did recognize that the terms of the contract may be a factor in determining whether a person had a reasonable expectation of privacy in the internet subscriber information.
- [40] The accused also referred to *R. v. Duarte*, [1990] 1 S.C.R. 30. In that case, the police with the assistance of an informer set up an undercover operation. They rented a room which was equipped with electronic recording devices. In that room, they conducted a discussion of a drug transaction with the accused. The transaction was recorded. The police had not obtained a warrant to make this recording, although they could have done so. The Crown argued that s. 178.11 (2)(a) of the Criminal Code at that time provided that it was not an offence to record the conversation provided the intended recipient or the originator of that communication consented beforehand. The Supreme Court of Canada however, found that although it may not be an offence, it was still an infringement of a person's rights to be free from unreasonable search and seizure. The Court found that Part IV.1 of the Criminal Code allowed this procedure if a warrant was obtained. The Court found that prior judicial authorization struck a reasonable balance between the rights of individuals to be left alone and the right of the state to intrude on privacy in order to enforce the law. However, the completely unregulated or unrestricted recording of conversations with the consent of one

of the participants was constitutionally invalid because it breached the right to protection against unreasonable search and seizure. The Court recognized that one of the participants could give oral testimony about the conversation, but that did not justify the surreptitious recording of such conversation. The Court said at para. 28:

...the assessment whether the surreptitious recording trenches on a reasonable expectation of privacy must turn on whether the person whose words were recorded spoke in circumstances in which it was reasonable for that person to expect that his or her words would only be heard by the persons he or she was addressing. As I see it, where persons have reasonable grounds to believe their communications are private communications in the sense defined above, the unauthorized surreptitious electronic recording of those communications cannot fail to be perceived as an intrusion on a reasonable expectation of privacy.

[41] The court recognized the risk that the listener may repeat our words, but distinguished that from the risk that the words may be recorded. The Court said at para. 30:

30. I am unable to see any similarity between the risk that someone will listen to one's words with the intention of repeating them and the risk involved when someone listens to them while simultaneously making a permanent electronic record of them. These risks are of a different order of magnitude. The one risk may, in the context of law enforcement, be viewed as a reasonable invasion of privacy, the other unreasonable. They involve different risks to the individual and the body politic. In other words, the law recognizes that we inherently have to bear the risk of the "tattletale" but draws the line at concluding that we must also bear, as the price of choosing to speak to another human being, the risk of having a permanent electronic recording made of our words.

[42] The Court also said at para. 32:

32 In summary, the question whether to regulate participant surveillance cannot logically be made to turn on the expectations of individuals as to whether their interlocutor will betray their confidence. No justification for the arbitrary exercise of state power can be made to rest on the simple fact that persons often prove to be poor judges of whom to trust when divulging confidences or on the fact that the risk of divulgation is a given in the decision to speak to another human being. On the other hand, the question whether we should countenance participant surveillance has everything to do with the need to strike a fair balance between the right of the state to intrude on the private lives of its citizens and the right of those citizens to be left alone.

[43] The Court then went on at para. 50 to state the following:

50 To conclude, the Charter is not meant to protect us against a poor choice of friends. If our "friend" turns out to be an informer, and we are convicted on the strength of his testimony, that may be unfortunate for us. But the Charter is meant to guarantee the right to be secure against unreasonable search and seizure. A conversation with an informer does not amount to a search and seizure within the meaning of the Charter. Surreptitious electronic interception and

recording of a private communication does. Such recording, moreover, should be viewed as a search and seizure in all circumstances save where all parties to the conversation have expressly consented to its being recorded. Accordingly the constitutionality of "participant surveillance" should fall to be determined by application of the same standard as that employed in third party surveillance, i.e., by application of the standard of reasonableness enunciated in *Hunter v. Southam Inc.*, *supra*. By application of that standard, the warrantless participant surveillance engaged in by the police here was clearly unconstitutional.

- [44] The Supreme Court of Canada in *Duarte* was concerned about a wide ranging power that would allow the police simply on their own and without any prior authorization or even the need for reasonable grounds, to record any and all communications by any and all members of the public that they chose.
- [45] The accused refers to *R. v. Kwok*, [2008] O.J. No. 2414, for the proposition that this also applied to internet chat logs. The issue in *Kwok* was whether electronic communication which took place in a private chat room was protected by a reasonable expectation of privacy and therefore its recording was contrary to the Charter.
- [46] It is not necessary for me to decide whether *Kwok* is correct. In *Kwok* an undercover police officer had communications with the accused in a public chat room. These communications did not carry a reasonable expectation of privacy because of the broad audience that could view them. However, the undercover officer then entered into communications with the accused in a private chat room where they were the only two individuals that view the chats. The computer being used by the undercover officer automatically recorded the contents of these chats. The court took the position that it was possible that the computer software could be set so that the chats would not be recorded. The trial judge felt that this was an important distinction and that such recording was contrary to decision in *Duarte*.
- [47] In our case the issue is not the recording of the chat messages, but the fact that Detective Krawczyk viewed those chats, which were intended for Quail. In our case, the chats were viewed by accessing Quail's account and not by accessing Mr. Caza's computer or anything attached to it.
- [48] In *Kwok*, the chats were simultaneous or live. However, as distinguished from verbal communication, this communication was in electronic form. It would be recorded on the computer receiving the chats and displayed on a screen. The data however, must be present before the information can be viewed. This is distinct from verbal or audio communication through the air. This is also distinct from a telephone conversation where the data is converted to sound waves rather than to an electronic image. The data must be entered on the hard drive before the computer can display it.
- [49] The accused's argument in the present case is that the sender had a reasonable expectation of privacy in any chat messages which were forwarded to Quail's account. However, those chat messages were preserved by the GigaTribe software which was used to send them until Quail accessed his account. Once the sender had sent them out, he lost all control over that

information and the data which formed that information. This is quite distinct from the surreptitious recording of conversations or communications between individuals. I would also add that the accused does not admit that he sent the chat messages. The chat messages were viewable without any access to the accused's computer or computer equipment. If his position is that the messages were sent by somebody else, using his computer equipment, he would still have no reasonable expectation of privacy in these chat messages himself. Even if his position was that he sent the chat messages and expected them to be read only by Devthedude2008, he would still have no reasonable expectation of privacy in those chats. These chats are similar to a letter or document sent to and placed in the control of a third party. The sender has given up all control over those documents. The police executing a search of the recipient's home, which entitles them to search documents as well, would be acting lawfully if they looked at the documents or in this case the chat messages.

- [50] The accused argues that there is a reasonable expectation of privacy in the internet subscriber information and referred to the *Cuttell* decision, however, in that case the court had no information about the contract between the internet service provider and the account holder. In the present case, the contract between the internet service provider and the account holder is in evidence and similar to the case of *R. v. McNeice*, 2010 BCSC 1544. *McNeice* was decided in November, 2010. The internet subscriber information in that case came from Northwestel. The court considered *Kwok* and *Cuttell* in which there was no evidence as to the particular terms of the contract between the user and the internet service provider. The court concluded that the terms of Northwestel made it clear that an individual did not have a reasonable expectation of privacy with regard to the name and address of the account. The agreement prohibited the use of the internet connection for dealing with obscene communications. Such use would be a breach of the agreement. The agreement also allowed Northwestel to release customer information to comply with an investigation into any activity which may violate the terms of the agreement.
- [51] The court also concluded that an internet service provider ("ISP") who simply responds to a police request under the Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 (the "PIPEDA"), is not acting as an agent of the police or the state. (Para. 44.) I agree with that conclusion. The ISP is really in the position of any other member of the community who is simply asked for information from the police and then provides it. The request does not amount to a search. The court did not apply the reasoning in *Kwok* and *Cuttell*. In any event the court said at para. 48 and 49:

48 I agree with the reasoning in the Ontario Court of Justice cases cited to me by the Crown, namely: *R. v. McGarvie*, 2009 CarswellOnt 500 (Ont. C.J.), Halikoski J.; *R. v. Verge*, 2009 CarswellOnt 501 (Ont. C.J.), J.J. Kearney J.; *R. v. Ward*, 2008 ONCJ 355, 176 C.R.R. (2d) 90, Lalande J.; *R. v. Friers*, 2009 ONCJ 103, J.S. Nadel J.; and *R. v. Wilson*, [2009] O.J. No. 1067, 2009 CarswellOnt 2064 (Ont. S.C.J.), L.C. Leitch J.

49 Wilson concluded, contrary to Kwok, that Internet subscriber information limited to name and address was not biographical information that one can reasonably expect to be kept private from the state. The conclusion is set out in paras. 41 - 43 as follows:

- [41] However, more importantly, I respectfully disagree with the conclusion in Kwok that "personal information such as names and addresses of customers held by companies, in this case Rogers [which was the internet service provider], would tend to disclose intimate details of lifestyle and choices" (para. 35). I note that this conclusion was arrived at without the opportunity to consider the Roger's internet subscriber agreement, and on that basis, Ward and Friers distinguished Kwok.
- [42] In my view, the Applicant had no reasonable expectation of privacy in the information provided by Bell considering the nature of that information. One's name and address or the name and address of your spouse are not "biographical information" one expects would be kept private from the state. It is information available to anyone in a public directory and it does not reveal, to use the words of Sopinka J. in Plant "intimate details of the lifestyle and personal choices or decisions of the applicant". As Nadal J. observed in Friers at para. 24:

Account information, per se, reveals very little about the personal lifestyle or private decisions of the occupants of the defendant's residence other than they have chosen to have some form of internet connection installed in that residence. Moreover, the prevalence of wireless and handheld technology makes a particular address an even less significant fact so far as internet use is concerned, since that use is no longer tied to a land line tied to a particular address.

- [43] In addition, in this case the terms of the contract with the internet provider is one of the factors to be considered in assessing whether the asserted expectation of privacy is reasonable in the totality of the circumstances. That contract includes an agreement that the service provider could disclose any information necessary to satisfy any laws, regulations or other governmental request from any applicable jurisdiction. Further, the agreement contained a provision that by subscribing to the service, one consents to the collection, use and disclosure of personal information as described in the Bell Customer Privacy Policy and the Bell Code of Fair Information Practices. This privacy statement includes a provision that Bell Canada may also provide personal information to law enforcement agencies. Therefore by virtue of the contractual terms on which the internet service was provided an expectation of privacy is not reasonable.
- [52] The Crown also referred to R. v. Ewanyshyn, (05 March 2009), Calgary 070764816Q1. In that case the court found that there was no reasonable expectation of privacy in an IP address. (Para. 21.) In that case, the ISP was Shaw and the court referred to the terms of the agreement with Shaw, which allowed Shaw to provide information to the police. (Para. 43.) The court also found that the name, address and phone number attached to the user account provided little biographical core information. (Para. 45 and 46.) In addition, there was no intrusion on to any place controlled by the accused, because the documents were in the control of a third party. (Para. 48.) The court found that even if there was a subjective

expectation of privacy, there was no reasonable expectation of privacy objectively. (Para. 51.)

- [53] The court also referred to *R. v. Brousseau*, 2010 ONSC 6753. This involved an ISP, Rogers. The court considered the terms of the contract between Rogers and the customer. The court concluded that these terms did allow the provision of a name, address and telephone number. The court concluded that name, address and telephone number did not disclose core biographical information. (Paras. 32 - 37.) The court also considered the PIPEDA in support of the proposition that there was no objective reasonableness to an expectation of privacy in this information in the hands of third parties. The court found that the police officer in execution of his duty to investigate crime, can send a letter of request for account information when they are investigating child exploitation. They are acting in the lawful execution of their duty. PIPEDA grants authority then for the ISP to disclose the information that it has collected for the purposes of assisting in the investigation without the requirement of a court order. (Paras. 38 - 44.) The court also found that the request was not a warrantless search as argued. (Para. 45.)
- [54] In a recent decision *R. v. Ballendine*, 2011 BCCA 221, our Court of Appeal dealt with the issue of PIPEDA beginning at para. 71 through para. 82. In that case, the police did obtain customer account information from Uniserve an ISP. The court did not have any information about the contractual terms with Uniserve and the accused. It was not possible on the record to determine whether PIPEDA applied to Uniserve. The court at para. 76 referred to McNeice. They did not confirm McNeice nor did they make any comment that would indicate that McNeice was incorrect in any way. The court found that the accused bore the onus of establishing that PIPEDA applied to the police requests and that Uniserve's responses to those request resulted in a breach of his Charter rights. He did not provide the evidence to resolve that and therefore his objection failed.
- [55] I accept Crown's argument that there is no reasonable expectation of privacy in the IP address. (*R. v. Wilson*, [2009] O.J. No. 1067.)
- [56] I also accept the Crown's arguments that the terms of the contract between Shaw and the holder of the account make it clear that the holder of the account had no reasonable expectation of privacy with regard to his name and address where the police are making the request pursuant to PIPEDA. The joint terms of service and acceptable use policies and privacy policies were exhibited before me. The terms of service are subject to the Shaw acceptable use policies, and allow Shaw to disclose any information necessary to satisfy any legal regulatory or other governmental request. The acceptable use policy allows Shaw to cooperate with law enforcement authorities in the investigation of suspected criminal violations. This includes Shaw providing a user name, IP address or other identifying information about the subscriber. The privacy policy that is part of the Shaw agreement does refer to PIPEDA.

- [57] The accused argues that the unreasonable search occurred on January 6, 2010, when Detective Krawczyk used Quail's account to download information that Paper123boy offered to share with Quail as one of his contacts. Again, it is not the recording of this information that is at issue, but the fact that it was downloaded. The argument is that this amounted to a search of Mr. Caza's computer or the hard drive attached to it at the time.
- [58] The accused argues that it is obvious there is a high expectation of privacy expected by the people using the GigaTribe software. He points out that this is a peer-to-peer network software designed to allow individual users to choose who they will share files with. The accused also points out that all communications or file transfers through the GigaTribe software are encrypted while they are being transferred from one computer to another. The accused argues that the nature of the software allows users to decide who they will share files with, in other words, who will be on their contact list and who will not. It allows them to remove a contact at any time and for any reason. Both users must agree to the contact relationship.
- [59] The accused argues that this demonstrates that a user expects that any information they share or any access they allow to files on their folder will only be exercised by their contacts. The accused argues that although they may not know the individual identity of their contacts, the use of the chat services allows users to recommend that others accept or reject certain contacts and through these communications and allows them to learn what other users might be good sharers.
- [60] The accused also argues that the appearance of the GigaTribe website and software does not indicate that it is being used for any illegal purpose. To a viewer it would simply be a private and secure means of exchanging any kind of electronic material. He argues that this indicates that a person using GigaTribe would have a very reasonable expectation of privacy. In other words, the documents would only be seen by the individuals that they selected.
- [61] The accused argues that if I were to conclude that there was not a reasonable expectation of privacy in these circumstances, that it could be detrimental to the legitimate use and development of this type of software or this particular software.
- [62] Counsel are in agreement on the general principles of the law dealing with applications under ss.8 and 24(2). Those principles are stated in *R. v. Edwards*, [1996] 1 S.C.R. 128. That case dealt with an accused charged with drug offences. The drugs were found at his girlfriend's apartment. The court found that he did not have any s. 8 protection respecting the search of the girlfriend's apartment. Referring to the decision *Canada (Combines Investigation Act, Director of Investigation and Research) v. Southam Inc.* [1984] 2 S.C.R. 145, the court in *Edwards* said the following at para. 30 and 31:

30 While Dickson J. advocated a broad general right to be secure from unreasonable search and seizure, he stressed that it only protected a "reasonable expectation of privacy". He stated at pp. 159-60 that the limiting term "reasonable" implied that:

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

31 It has since been determined that this assessment must be made in light of the totality of the circumstances of a particular case. See, for example, *R. v. Colarusso*, [1994] 1 S.C.R. 20, at p. 54, and *R. v. Wong*, [1990] 3 S.C.R. 36, at p. 62.

[63] The court also said at para. 33:

33 It is important to emphasize that generally, the decision as to whether an accused had a reasonable expectation of privacy must be made without reference to the conduct of the police during the impugned search. There are two distinct questions which must be answered in any s. 8 challenge. The first is whether the accused had a reasonable expectation of privacy. The second is whether the search was an unreasonable intrusion on that right to privacy. See *Rawlings v. Kentucky*, 448 U.S. 98 (1980). Usually, the conduct of the police will only be relevant when consideration is given to this second stage.

[64] In dealing with s. 8 the court said at para. 45:

45 A review of the recent decisions of this Court and those of the U.S. Supreme Court, which I find convincing and properly applicable to the situation presented in the case at bar, indicates that certain principles pertaining to the nature of the s. 8 right to be secure against unreasonable search or seizure can be derived. In my view, they may be summarized in the following manner:

1. A claim for relief under s. 24(2) can only be made by the person whose Charter rights have been infringed. See *R. v. Rahey*, [1987] 1 S.C.R. 588, at p. 619.
2. Like all Charter rights, s. 8 is a personal right. It protects people and not places. See *Hunter*, *supra*.
3. The right to challenge the legality of a search depends upon the accused establishing that his personal rights to privacy have been violated. See *Pugliese*, *supra*.
4. As a general rule, two distinct inquiries must be made in relation to s. 8. First, has the accused a reasonable expectation of privacy. Second, if he has such an expectation, was the search by the police conducted reasonably. See *Rawlings*, *supra*.
5. A reasonable expectation of privacy is to be determined on the basis of the totality of the circumstances. See *Colarusso*, *supra*, at p. 54, and *Wong*, *supra*, at p. 62.
6. The factors to be considered in assessing the totality of the circumstances may include, but are not restricted to, the following:
 - (i) presence at the time of the search;
 - (ii) possession or control of the property or place searched;

- (iii) ownership of the property or place;
- (iv) historical use of the property or item;
- (v) the ability to regulate access, including the right to admit or exclude others from the place;
- (vi) the existence of a subjective expectation of privacy; and
- (vii) the objective reasonableness of the expectation.

See *United States v. Gomez*, 16 F.3d 254 (8th Cir. 1994), at p. 256.

7. If an accused person establishes a reasonable expectation of privacy, the inquiry must proceed to the second stage to determine whether the search was conducted in a reasonable manner.

[65] The Supreme Court of Canada also dealt with reasonable expectation of privacy in the case *R. v. Tessling*, [2004] 3 S.C.R. 432. The *Tessling* case dealt with forward looking infrared technology, which was used to detect the heat signal emanating from a building. The question was, whether this amounted to an unreasonable search. The heat signal was useful in determining the possibility or probability that there was marijuana grow operation located in the building. The Court looked at the totality of the circumstances in determining whether this amounted to an unreasonable search. The Court said at para. 32:

- (1) Did the Respondent Have a Reasonable Expectation of Privacy?

32 On the facts of this case, we need to address:

1. What was the subject matter of the FLIR image?
2. Did the respondent have a direct interest in the subject matter of the FLIR image?
3. Did the respondent have a subjective expectation of privacy in the subject matter of the FLIR image?
4. If so, was the expectation objectively reasonable? In this respect, regard must be had to:
 - a. the place where the alleged "search" occurred;

[page 448]

- b. whether the subject matter was in public view;
 - c. whether the subject matter had been abandoned;
 - d. whether the information was already in the hands of third parties; if so, was it subject to an obligation of confidentiality?
 - e. whether the police technique was intrusive in relation to the privacy interest;
 - f. whether the use of surveillance technology was itself objectively unreasonable;

- g. whether the FLIR heat profile exposed any intimate details of the respondent's lifestyle, or information of a biographical nature.

[66] Both counsel also referred to the Supreme Court of Canada decision *R. v. Plant*, [1993] 3 S.C.R. 281. The *Plant* case involved the police obtaining information about electrical consumption related to a specific residential address. They obtained this from the electrical utilities computer. The evidence about the rate of consumption was part of the information relied on in the information to obtain a search warrant regarding the residence. In dealing with computerized records, the Court said the following:

16 The purpose of s. 8 is to protect against intrusion of the state on an individual's privacy. The limits on such state action are determined by balancing the right of citizens to have respected a reasonable expectation of privacy as against the state interest in law enforcement. See *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at pp. 159-60. Section 8 protects people and not property. It is, therefore, unnecessary to establish a proprietary interest in the thing seized. See *Hunter*, *supra*, at p. 158; *R. v. Dyment*, [1988] 2 S.C.R. 417, per La Forest J., at pp. 426-27; *Katz v. United States*, 389 U.S. 347 (1967). [page292] In this respect, I must disagree with the Court of Appeal which relied on the absence of a proprietary interest on the part of the appellant in the computer information.

17 In balancing the reasonable expectation of privacy of the individual with the interests of the state in law enforcement, this Court has determined that electronic taping of private communication by state authorities violates the personal sphere protected by s. 8: *R. v. Duarte*, [1990] 1 S.C.R. 30. Similarly, such investigative practices as videotaping of events in a private hotel room (*R. v. Wong*, [1990] 3 S.C.R. 36) and seizure by state agents of a blood sample taken by medical personnel for medical purposes (*Dyment*, *supra*) have been found to run afoul of the s. 8 right against unreasonable search and seizure in that the dignity, integrity and autonomy of the individual are directly compromised. While this Court has considered the possibility of violations of s. 8 in relation to informational privacy (*Dyment*, *supra*, at p. 429), we have not previously considered whether state inspection of computer records implicates s. 8 of the Charter.

18 Some indication of the parameters of the protection afforded by s. 8 with respect to informational privacy can be derived from the following passage from the reasons of La Forest J. in *Dyment*, *supra*, at pp. 429-30, commenting on the Report of the Task Force on Privacy and Computers:

In modern society, especially, retention of information about oneself is extremely important. We may, for one reason or another, wish or be compelled to reveal such information, but situations abound where the reasonable expectations of the individual that the information shall remain confidential to the persons to whom, and restricted to the purposes for which it is divulged, must be protected.

[page 293]

19 Consideration of such factors as the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated allows for a balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement. It is, then, necessary to apply this contextual approach to the facts of the case at bar.

20 The United States Supreme Court has limited application of the Fourth Amendment (the right against unreasonable search and seizure) protection afforded by the United States Constitution to situations in which the information sought by state authorities is personal and confidential in nature: *United States v. Miller*, 425 U.S. 435 (1976). That case determined that the accused's cheques, subpoenaed for evidence from a commercial bank, were not subject to Fourth Amendment protection. While I do not wish to be taken as adopting the position that commercial records such as cancelled cheques are not subject to s. 8 protection, I do agree with that aspect of the *Miller* decision which would suggest that in order for constitutional protection to be extended, the information seized must be of a "personal and confidential" nature. In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the Charter should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual. The computer records investigated in the case at bar while revealing the pattern of electricity consumption in the residence cannot reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence.

[67] The Court found that the relationship between the appellant and the utility commission was not one of confidence (para. 21) and there was no evidence that it was contractually bound to keep the information confidential. The transaction records maintained as a result of the commercial relationship between the utility company and the appellant was not a confidential communication. (Para. 22.) The Court also noted that a member of the public could request the energy consumption at a particular address, although that was not determinative of the issue. (Para. 22.)

[68] The information was obtained from the utility company and not by intrusion into a place ordinarily considered private or an invasion of personal computer records confidentially maintained by a private citizen. (Para. 23) The Court also said at para. 24:

24 In addition to the fact that the manner and place of the search are indicative of a minimally intrusive search, the seriousness of the offence militates in favour of the conclusion that the requirements of law enforcement outweigh the privacy interest claimed by the appellant. As this Court previously concluded in *Kokesch*, supra, while participation in the illicit trade of marihuana may not be as serious as the trade in other narcotics such as cocaine, it remains an offence which is taken seriously by law enforcement agents.

25 Overall, I have concluded from the nature of the information, the relationship between the appellant and the Commission, the place and manner of the [page296] search and the seriousness of the offence under investigation, that the appellant cannot be said to have held a reasonable expectation of privacy in relation to the computerized electricity records which outweighs the state interest in enforcing the laws relating to narcotics offences. As such, the appellant has failed to bring this search within the parameters of s. 8 of the Charter. This information was, therefore, available to the police to support the application for a search warrant. I will consider, next, the sufficiency of the information in support of the issue of the search warrant.

The Defence Position

[69] The defence argues that when Detective Krawczyk accessed the GigaTribe account and downloaded information from the Paper123boy account he was conducting a search of the computer used by Paper123boy. The defence argues that he did this by using access granted to another individual, that is Quail, and viewed private communications intended for Quail. He argues that this ignored any privacy interests that the accused might have and therefore he was not acting in good faith.

[70] He analyzed the expectation of privacy and argued that it was particularly high. He used the analysis in the *Cuttell* case which is essentially that from the Supreme Court of Canada decisions. The factors that he argued were as follows:

1. the subject matter of the search was the 500 gigabyte hard drive found by the police in the accused's residence and used by Paper123boy. This was available to the contacts of Paper123boy, but not others.
2. the hard drive was found in Mr. Caza's residence. The evidence shows that it was purchased by Mr. Caza.
3. Mr. Caza had a subjective expectation of privacy in the hard drive, because it was found in his residence and had been connected to his personal computer.

[71] The defence argues that this expectation of privacy was objectively reasonable on the following basis:

- a. The hard drive was attached to the GigaTribe network and only available to contacts of Paper123boy.
- b. The subject matter was not in plain view because it could only be viewed by contacts.

- c. The hard drive and the information available had not been abandoned.
 - d. The information was not in the hands of a third party was on the hard drive connected through the GigaTribe network.
 - e. The IP address was discovered by downloading information from the hard drive and the account information was in the hands of Shaw, but the defendant argues subject to an understanding of confidentiality, the police investigation was intrusive in that it used access authorized by specific individuals, and not the detective who downloaded the information.
 - f. The search exposed intimate details of the applicant's lifestyle of information of a biographical nature, because it showed communications with groups or individuals interested in child pornography.
- [72] The accused also argues there was no urgency or exigent circumstances.

The Crown's Position

- [73] The Crown argues that Detective Krawczyk was not involved in a warrantless search when he accessed information through the GigaTribe account. The Crown draws comparisons to cases where evidence has been abandoned or there has been a voluntary exposure of information. The Crown also argues that this was a legitimate police technique involving a subterfuge, that is going under cover or representing themselves as somebody else, that those techniques do not constitute searches.
- [74] The defence argues that the very nature of the GigaTribe peer-to-peer software indicates a high expectation of privacy because of the limited contacts who can access information, which are files offered to be shared and the encryption.
- [75] The Crown points to the nature of the GigaTribe software and the evidence that the users go to great lengths to maintain their anonymity and give control of communications and data to other anonymous users.
- [76] The defence raises no issues with the manner in which Detective Krawczyk obtained the user name and password for Quail's GigaTribe account.
- [77] Access to Quail's GigaTribe account allowed detective Krawczyk to see Quail's list of online list of contacts, messages, folders and data, which were being offered to Quail for the purposes of sharing.
- [78] The Paper123boy account attracted attention because of the messages which had been broadcast to Quail and were viewable by Detective Krawczyk without Detective Krawczyk having to access the computer used by Paper123boy.

- [79] The messages may have been intended for Quail or other contacts of Paper123boy, but were no longer under the control of Paper123boy once they had been posted through the GigaTribe software. They were now available to Quail or anyone who had access to his account.
- [80] I note that I have been using Mr. Quail's name in reference to his account, but there is no evidence that Paper123boy or the accused had any personal relationship with Quail or knew who he was. The only evidence available indicates that Quail's contacts would know him by his user name Devthedude2008, but not otherwise.
- [81] The evidence of Detective Krawczyk is that he has investigated thousand of GigaTribe accounts and internet child pornography sites and exchanges. It is possible that the users of GigaTribe may know each other from other chat sites or message sites and then agree to meet on GigaTribe. He is not aware of any instance in which the users knew each other or had any personal information about each other. In fact, based on his investigations, there is little or no discussion about any personal or identifying details between users, and if it comes up the information provided is fictional. The users are concerned with anonymity and avoiding detection. In addition, the users who may be attempting to exploit children on the internet, seldom disclose who they are, but rather represent themselves as someone else or fictional characters. Subterfuge and disguise are commonly used by people attempting to exploit children on the internet. They are attempting to disguise their identity from the people that they are exploiting. It would be clear to anybody in that position that they have no more assurance about who was on the other end of the computer connection than that person has about who they are.
- [82] Paper123boy was using the premium or ultimate version of the GigaTribe software. They designated the files they offered to share as "read only". One of the contacts, who wished to access or share that folder, would click on folder to preview it and download it. The contact had no ability to change or alter anything on the folder, nor did they have any other access to any other file or portion of Paper123boy's computer. They could look at and download the file being offered, but they could not search or obtain any data from Paper123boy's computer in any other fashion. I also note that the accused does not assert any knowledge or interest in the particular files which were accessed by Detective Krawczyk.
- [83] The Crown argues that the software technology does not provide any user with an assurance that their data or communications would remain private once it had been accessed by that person's contacts. In addition, the GigaTribe program could be left to run automatically. In other words, Paper123boy did not have to be at the computer. In fact, some of the chat messages ultimately obtained from the hard drive indicate that this was something that Paper123boy did on occasion. This would allow any of the contacts to download the files that were being offered for sharing.

- [84] The Crown also argues that the very anonymity, which is provided by the software and a part of the sub culture of child pornography for sharing the files, is a factor to consider in the expectation of privacy. The users seek anonymity and do whatever they can to prevent anybody from learning their true identity. In that environment, the user has no idea who they are actually dealing with. The user of this software can decide who will be their contacts and what to share with those contacts. However, the evidence is that it is extremely unlikely they would have any personal knowledge about who the contact actually was. In other words, all they know is that they are dealing with a user name on an account affiliated with the same software. They have no idea who is behind that user name. They do not know whether it is a man, a woman, more than one person, someone else interested in child pornography or police officers investigating child pornography offences. They have no way of knowing whether the individual or individuals behind the user name changes at any time.
- [85] They may, as a result of the chat feature, believe they have developed some understanding or relationship with various contacts. They may sense a change in the behaviour of one of the contacts or for any particular reason may decide they no longer feel secure or willing to share with that contact and eliminate that contact. In fact, Paper123boy eliminated Devthedude2008 as a contact on January 8, 2010. However, there is no way of knowing whether that may have been as a result of some information received or merely a reaction to some perceived change in behaviour. This is certainly not any evidence of any knowledge of what lies behind the username Devthedude2008.
- [86] The user of this GigaTribe software in the circumstances of the child pornography exchange is motivated to accept contacts in the hope that they will benefit from that contact by the exchange of child pornography. They may even hope to engage in communications with other people interested in child pornography, to be part of a community of some sort. However, they would know that there is no way that they can be assured of what or who lies behind the user name. They hope that the person or people behind the name share their interests and that they are not dealing with a police officer who is essentially acting under cover.
- [87] All they can really know when they chose to accept a contact is that they are choosing to share information or files with anyone who has access to that user's account through their username and password. They have no way of controlling who that might be or even knowing where in the world that person or people may be accessing the account from.
- [88] Detective Krawczyk compared this to a masquerade ball. People put on costumes and attend the party. They may come and go, and somebody else may assume their costume. No one knows who they are dealing with or even if it is the same person in the costume from time to time.
- [89] Detective Krawczyk gave an example of the difficulty of knowing who is behind the internet connection. He was teaching a course to other policeman. During his discussions he connected his computer to the internet and displayed the screen on a large screen, so that

everybody in the room could observe it. He then made contact with an individual he knew to be interested in exploiting children. He represented himself as a 13 year old girl and entered into a chat discussion with the individual on the other end. After several compromising things were communicated by the person on the other end, Detective Krawczyk dropped the ruse of being a 13 year old girl and thanked the individual for helping in the education of a number of police officers. The user on the other end immediately disconnected.

- [90] The Crown refers to the decision *R. v. Friers*, 2008 ONCJ 740. In that case the accused had provided four photographs to an undercover police officer through the internet. These photographs were child pornography and the police were able to obtain an IP address and account information and a search warrant for the home. The police searched the computer and found two additional pieces of child pornography. In that case the police had arrested an administrator of a chat room, dedicated to child pornography. Detective Krawczyk was able to masquerade as that administrator on the internet. The chat room software provided the administrator with IP addresses of everyone accessing the chat room. The accused, that Detective Krawczyk was communicating with, went by various pseudonyms in order to hide his identity. The decision dealt with the release of the internet service account information without a warrant. The court found that did not result in a s. 8 breach. The court dealt with reasonable expectation of privacy in the chat room at para. 26 where the court said:

The defendant was content to correspond with parties unknown to him in chat-rooms and on programmes that he did not control. The defendant, I find, had no reasonable expectation of privacy in those communications. That is why he attempted to hide his identity behind pseudonyms. He had no reasonable expectation that his contacts through these chat-rooms and programmes would be private communications. He offered his vile inventory to any who wished to browse and download it on the occasions outlined in the evidence.

- [91] The software in this case, does allow a person to restrict the contacts that they have and the people who can access the information they make available. In this case, Paper123boy had 85 contacts. This is not the same as many forms of peer-to-peer software, which allows all of the people using that software to access any files being offered for sharing by anybody else in the group. However, the fact that a user has no idea in reality who they are offering to share with is an important factor in determining whether there is realistically any reasonable expectation of privacy. There is a hope for, but no objectively realistic expectation of privacy.
- [92] The Crown also points to evidence in the chat messages which indicate that the users are aware of the risk that their communications may not be private. Clearly the users are aware and Paper123boy was aware that despite attempts at anonymity, data could be exposed or accessed by others whenever the computer was on and GigaTribe was running. There was a hope that other contacts would be careful, but the chats indicate that there was no assurance of that. One of the messages indicated that some of the users list their own users in their shared folders and that this was not safe. Paper123boy acknowledged that message saying that he never posted user lists. This was in messages in late December, 2009. There

were also chat messages asking for verification as to whether the people who were seeking to be included in contacts were safe and Paper123boy replied that he did not know them and that person should be careful. This again indicates that there is a risk of accepting a contact, that your identity may be compromised if either the contact's identity is compromised or the contact is not reliable or careful.

- [93] The Crown correctly argues that a user who accepts a contact is really taking a chance that they may be exposed. They have no idea who the contact is or where that contact is located. They have no idea what the laws might be in the jurisdiction in which that contact may be located and they have no way of knowing or controlling that contact's behaviour. As pointed out by Detective Krawczyk, they do not know whether the contact is viewing shared files on the account on a computer sitting in a public place or with other people present. They also have no assurance that the information contained in the other users computer, including their password, may not fall into the hands of investigators in whatever jurisdiction that user is located and may then come into the possession of investigators in Canada.
- [94] The defence used the analogy of a house key or an owner of property who allowed access to other individuals to their property. They argued that Paper123boy could control who had access to the files that he offered to share. The fact that he had given access to Devthedude2008 did not authorize the police using Devthedude2008's account to have the same access. He argued that it was like giving the key to your home to a friend. If the friend is arrested, and the police find the key, they are not entitled to enter your home. Defence counsel properly acknowledged the difficulty of using analogies and saying one thing is like another, does not mean that it is the same as another.
- [95] I do not find the house key or the property analogy useful in this case. In this case, what has happened is that Paper123boy has sent out a message on the internet to his contacts saying you can access this information by clicking on it. A closer analogy would be a drug dealer phoning one of his customers. The customer has just been arrested by the police and a police officer picks up the phone. The drug dealer says: I have your drugs and I will meet you at a certain location. The police officer simply responds by saying, I will be there. The police then attend at the location and arrest the drug dealer. When Detective Krawczyk clicked on the file being offered, it was like it was he answering the phone. However, in this case, Paper123boy had gone further in putting the information beyond his control, by allowing it to be accessed by anybody with access to his contacts accounts without Paper123boy having to do anything further.
- [96] The Crown in its argument referred to the Edwards decision as an analogy. That dealt with an accused drug dealer who left drugs in his girlfriend's apartment. The court found that he had no reasonable expectation of privacy in that apartment. This was because he had no control over people who came and went. The analogy is not particularly helpful in this case. Here, the argument is that the files were on the hard drive attached to the accused's computer. However, as I pointed out earlier, the accused makes no claim to any interest in the files themselves.

Finding a Balance

[97] The Crown argues that the present reality of computer technology and the internet must be considered in determining where the balance should be drawn about a person's reasonable expectation in the use of software such as GigaTribe. The Crown refers to the on-line virtual communities and the volumes of anonymous file sharing and proliferation of internet crime, including child pornography.

[98] The Crown refers to Tessling at paras. 17 and 18:

A. Striking the Balance

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

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

18 The notion of the "balance" was also canvassed by Sopinka J. in advocating a "contextual approach" in *R. v. Plant*, [1993] 3 S.C.R. 281, at p. 293:

Consideration of such factors as the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated allows for a balancing of the societal interests in protecting individual dignity, integrity and autonomy with effective law enforcement.

In the result the right to be free from examination by the state is subject to constitutionally permissible limitations. First, "not every form of examination conducted by the government will constitute a 'search' for constitutional purposes. On the contrary, only where those state examinations constitute an intrusion upon some reasonable privacy interest of individuals does the government action in question constitute a 'search' within the meaning of s. 8"; *Evans*, supra, at para. 11. It is only "[i]f the police activity invades a reasonable expectation of privacy, [that] the activity is a search"; *R. v. Wise*, [1992] 1 S.C.R. 527, at p. 533. Second, as the language of s. 8 implies, even those investigations that are "searches" are permissible if they are "reasonable". A search will not offend s. 8 if it is authorized by a reasonable law and carried out in a reasonable manner: *R. v. Caslake*, [1998] 1 S.C.R. 51; [page443] *R. v. Collins*, [1987] 1 S.C.R. 265.

[99] The Crown then refers to para. 40 of Tessling:

40 It is true that a person can have no reasonable expectation of privacy in what he or she knowingly exposes to the public, or to a section of the public, or abandons in a public place (*R. v. Boersma*, [1994] 2 S.C.R. 488; *Stillman*, *supra*, at para. 62, per Cory J., and at para. 226, per McLachlin J. (as she then was), dissenting; *Evans*, *supra*, at para. 50, per Major J., concurring; *Baron v. Canada*, [1993] 1 S.C.R. 416, at p. 453; *Dyment*, *supra*, at p. 435; and *R. v. Monney*, [1999] 1 S.C.R. 652, at para. 45).

[100] Next the Crown refers to the issue of abandonment in determining a reasonable expectation of privacy and refers to *R. v. Patrick*, 2009 S.C.C. 17. In *Patrick*, the Court was dealing with information the police obtained from the garbage that the accused had placed on the edge of his property in the alley for pick up. The Court had essentially said that when a person gives up control of information or evidence in those circumstances where any member of the public could have access to it, they can have no reasonable expectation of privacy.

[101] The Crown is not suggesting that Paper123boy has abandoned the files that he has offered to share. However, the Crown's argument is that similar to abandonment in this case, he has given up control of those files to the other users on his contact list. He has no real knowledge of who those contact might be, therefore can have no real expectation of privacy in the files he has offered to share.

[102] The Crown refers to three American cases that deal with the GigaTribe software. In those cases an undercover investigator took over the account of a GigaTribe user and without warrant downloaded files containing child pornography. The accused in those cases argued that they had relied on GigaTribe's special features to prevent public access to the files and therefore had a reasonable expectation of privacy. The government argued that the person who had voluntarily shared files had no reasonable expectation of privacy in that information.

[103] In the case *United States v. Ladeau*, 2010 Dist. LEXIS 34218 (D. Mass. April 7, 2010), the court referred to cases dealing with other peer-to-peer software such as LimeWire in which it was held the accused did not have a reasonable expectation of privacy. The Court noted that *Ladeau* referred to the differences between that type of peer-to-peer software and the GigaTribe peer-to-peer software including the control over contacts. The court found that such security measures however do not establish that reasonable expectation of privacy was objectively reasonable.

[104] The court at page 8 of that decision said:

No matter how strictly *Ladeau* controlled who accessed his computer files, he had no control over what those people did with information about the files once he granted them access. The Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith*, 442 U.S. at 743-744.

- [105] In the decision *United States v. Sawyer*, 786 F. Supp. 2d 1352, 2011 U.S. Dist. LEXIS 57662 (N.D. Ohio May 25, 2011), the court again dealt with the issue of the GigaTribe software and reasonable expectations of privacy. In this case the court was referring to what then was described as the "friends list", which is the same as the contact list in our case. The police obtained permission of one of the users to use their password and through that ruse engage in a private chat with the accused. The police were able to obtain the IP address and then the internet service providers account information. The court essentially said that once you grant a person in the position of "friend" access, you have lost control over the manner in which the friend uses that access. The court said simply being able to designate people "friends" does not alter the fact that the user had then lost control of the files because they were no longer kept private. Because there was no control over what "friends" might do with the material, there could be no reasonable expectation of privacy.
- [106] That is even more significant in the circumstances where you do not know who the friends may be.
- [107] The third case is *United States v. Soderholm*, 2011 U.S. Dist. LEXIS 130727 (D. Neb. November 9, 2011). Again, the court found that despite the nature of a P2P network that allowed you to select your own contacts, the court found that the accused did not have a reasonable expectation of privacy for those files which he was sharing with "friends" on this private network. The files were no longer kept private and the accused could not control what the "friends" might do with the files.
- [108] I keep in mind that in the U.S.A. cases they were dealing with "Fourth Amendment protection", as provided by the Constitution of the U.S.A.
- [109] The Crown also argues that in our case, Detective Krawczyk was involved in a ruse or acting in an undercover capacity and that this does not render the search, if it was a search, unlawful. Crown also argues that search, if it was a search, was not conducted in an unreasonable manner.
- [110] The Crown refers to *R. v. Roy*, 2010 BCCA 448. In that case the undercover police officers posed as drug dealers and gained access to the accused's home. The accused showed them money and drugs. The accused argued that the evidence should be excluded because this amounted to an unreasonable search. The court found that he had waived or abandoned any expectation of privacy and no s. 8 search or seizure occurred. (Para. 23.) The court recognized ones actions may alter the reasonable expectation of privacy one may have in one's residence (Para. 24.) The court then went on to find that the police were acting pursuant to the expressed invitation of the accused when they entered the home and were shown the drugs and money. The court found that the police could use the information that they obtained through an undercover operation such as that. This did not amount to a s. 8 search and seizure. The court also found that such conduct would not shock the community.

- [111] Detective Krawczyk was not actually undercover when he used Quail's account to access or download the files being offered by Paper123boy. However, I am satisfied that using the account is not conduct which would shock the community in any sense of the word. In this case there was no contact whatsoever with Paper123boy and no contact with the accused. The only thing Detective Krawczyk did was view and download files which Paper123boy had offered to share.
- [112] The Crown argues that the GigaTribe account is certainly a less private place than a physical dwelling house and that the access that was allowed to the computer hard drive was extremely limited. Crown also argues that the point of GigaTribe is to share information, not to keep it private and that the analogy to a home or physical place is simply not applicable in our search or circumstances. The Crown then argues that if Roy's expectation of privacy in his home was diminished through a ruse or an undercover operation, it did not amount to a s. 8 search, there is no reason to conclude that the police using the account of Devthedude2008, or essentially acting under cover, have conducted an unlawful search because they viewed files offered by Paper123boy.
- [113] In applying the guidelines referred to in Tessling and discussed at paras. 97 to 99 of this decision, the balance requires a finding that Detective Krawczyk was not conducting an unreasonable search when he viewed and downloaded the files offered by Paper123boy.

Conclusion

- [114] I find that Detective Krawczyk did not breach any of the accused's rights to be free from unreasonable search and seizure when he used Quail's GigaTribe account to view and download the files being offered for sharing by Paper123boy. By clicking on these thumbnails that were shown on Quail's GigaTribe account, he was merely accepting the offer to download that had been extended by Paper123boy to an anonymous contact. He did not search the hard drive to which those files resided. The accused makes no claim to any interest in those files, but only a claim to an interest in the hard drive in which they were stored. In all of the circumstances and for the reasons I have discussed above, I find that there was no reasonable expectation of privacy that the accused had in these particular files and the limited access to his hard drive did not amount to a search, which would be protected by s. 8 of the Charter.
- [115] I have also concluded that Detective Krawczyk did not breach any reasonable expectation of privacy the accused may have had in the IP address attached to the chat messages or the files when they were downloaded. I have also concluded that he had no reasonable expectation of privacy protected by the Charter in the information provided by the Shaw to Detective Krawczyk. The terms of the agreement support that conclusion.

- [116] The fact that the account was in the name of Brian Feltham and not in the name of the accused is not significant. The evidence is that the account was originally opened at the request of Brian Feltham when he resided at the accused's residence for a short time. The accused is the person who continued to use and pay for that account.
- [117] I find that the information obtained by Detective Krawczyk was properly included in the information to obtain the search warrant and the search warrant was properly issued.
- [118] The accused does not argue that the manner in which the search of the residence was conducted was unreasonable if it was pursuant to valid warrant. I am satisfied on the evidence that the manner in which the search was conducted was reasonable.

Charter s. 24(2)

- [119] Although I have concluded that there was no s. 8 breach, in the event that I am wrong I have considered whether the accused has proven on the balance of probabilities that the evidence obtained as result of the search should be excluded from the trial.
- [120] Section 24(2) provides:
- (2) Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this Charter, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.
- [121] Both counsel agree that the proper analysis is that established by the Supreme Court of Canada in *R. v. Grant*, [2009] 2 S.C.R. 353. I am referring to the Crown's submission and those portions of *Grant* that they have referred to as follows:

68 The phrase "bring the administration of justice into disrepute" must be understood in the long-term sense of maintaining the integrity of, and public confidence in, the justice system. Exclusion of evidence resulting in an acquittal may provoke immediate criticism. But s. 24(2) does not focus on immediate reaction to the individual case. Rather, it looks to whether the overall repute of the justice system, viewed in the long term, will be adversely affected by admission of the evidence. The inquiry is objective. It asks whether a reasonable person, informed of all relevant circumstances and the values underlying the Charter, would conclude that the admission of the evidence would bring the administration of justice into disrepute.

...

71 A review of the authorities suggests that whether the admission of evidence obtained in breach of the Charter would bring the administration of justice into disrepute engages three avenues of inquiry, each rooted in the public [page394] interests engaged by s. 24(2), viewed in a long-term, forward-looking and societal perspective. When faced with an application for exclusion under s. 24(2), a court must assess and balance the effect of admitting the evidence on

society's confidence in the justice system having regard to: (1) the seriousness of the Charter-infringing state conduct (admission may send the message the justice system condones serious state misconduct), (2) the impact of the breach on the Charter-protected interests of the accused (admission may send the message that individual rights count for little), and (3) society's interest in the adjudication of the case on its merits. The court's role on a s. 24(2) application is to balance the assessments under each of these lines of inquiry to determine whether, considering all the circumstances, admission of the evidence would bring the administration of justice into disrepute. These concerns, while not precisely tracking the categories of considerations set out in *Collins*, capture the factors relevant to the s. 24(2) determination as enunciated in *Collins* and subsequent jurisprudence.

The Seriousness of the Charter - Infringing State Conduct

[122] As pointed out in *Grant* and both counsel's submissions, the seriousness of the state conduct, which amounts to a Charter breach can be seen on a continuum from minor or technical errors to deliberate or negligent disregard for personal rights. (*Grant* at paras. 72 - 75) The court must determine whether the nature of the police conduct was such that the court must disassociate itself from that conduct. As the court stated in *Grant* at para 74:

74 State conduct resulting in Charter violations varies in seriousness. At one end of the spectrum, admission of evidence obtained through inadvertent or minor violations of the Charter may minimally undermine public confidence in the rule of law. At the other end of the spectrum, admitting evidence obtained through a wilful or reckless disregard of Charter rights will inevitably have a negative effect on the public confidence in the rule of law, and risk bringing the administration of justice into disrepute.

[123] The court did point out that ignorance of the Charter standards does not amount to good faith. (Para. 75.)

[124] The accused also refers to para. 75 in *Grant* that warns condoning or ignoring Charter breaches may have an impact on the general public and individuals not accused of crime:

It should also be kept in mind that for every Charter breach that comes before the courts, many others may go unidentified and unredressed because they did not turn up relevant evidence leading to a criminal charge. In recognition of the need for courts to distance themselves from this behaviour, therefore, evidence that the Charter-infringing conduct was part of a pattern of abuse tends to support exclusion.

[125] The accused says that this is of particular importance in this case because of the technology involved and the chilling effect that allowing the admission of this evidence might have on people who wish to use this technology for legitimate purposes.

- [126] The accused argues that Detective Krawczyk blatantly disregarded individual rights and privacies by examining files and information which was intended for only certain people including Devthedude2008. He argues that Detective Krawczyk obtained and used the access which was intended for Devthedude2008, without any knowledge of Paper123boy. He argues that there was no urgency or exigent circumstances.
- [127] The Crown in contrast argues that there was no flagrant, willful or reckless disregard for Charter rights. The Crown points out that at the time there did not appear to be any Canadian courts or American courts who have considered the nature of a GigaTribe peer-to-peer file sharing software. In fact, the law appeared to be that outlined in the Alberta court decision Ewanyshyn that dealt with the normal peer-to-peer software and concluded that there was no reasonable expectation of privacy in child pornography files unwittingly shared with a police officer. In that case, the police officer was able to access the accused's computer and browse through the child pornography files which were in the shared file.
- [128] The Crown points out that Detective Krawczyk obtained the password for Devthedude2008's account, by lawful means when the computer used by Devthedude2008 or Quail was seized in the United States. The Crown then says that really Detective Krawczyk was acting in an undercover capacity in the pursuit of evidence. The Crown argues that his conduct in this case was measured and would not shock the community. The Crown argues that he was operating in a virtual environment, which effectively required some level of deception in order to establish conduct with criminals. He simply used the access which was available to the user of the account Devthedude2008, which could have been anybody, and he did no more than look at the files being offered by Paper123boy. He did not search the computer; he merely looked at the files being offered. In fact, he had no access to any other part of the computer.
- [129] The Crown also points out that the only connection to the hard drive used by Paper123boy occurred on January 6, 2010, and Detective Krawczyk only viewed communications that were immediately viewable because they had been sent by Paper123boy and were held on the GigaTribe server or by the GigaTribe software. He had no control over the Paper123boy's computer and could do no more than Paper123boy had allowed him to do. This was not a free ranging or untrammelled state surveillance or interception as the kind warned of in Duarte. He only viewed the files which Paper123boy had offered to share and although these resided on a hard drive attached to the accused's computer. He did not take any steps to access any other portion of the hard drive at that time.

[130] The Crown argues:

in the more involved matters of GigaTribe and section 8 of the Charter, Detective Krawczyk stood, as the Court does now, at a place where complex lines of judicial authority, relating to such issues as privacy, state intrusion, conduct by an accused limiting privacy expectation, Charter limits and approved police tactics, all intersect and require some balance".

- [131] The Crown also points out that with regard to the law enforcement request for the internet service providers account information, that the process followed by the officer was consistent with additional authority at that time despite what was said in *Cuttell and Kwok*.
- [132] I agree with the Crown that in this case, if a breach occurred, it was not serious. There was no general access to the accused's computer or any material on that computer when the officer downloaded the files that were being offered for sharing or obtained the IP addresses.
- [133] The search of the residence which occurred subsequently, was certainly a serious intrusion into an individual's rights, but was done pursuant to a warrant, which the police believed they had obtained lawfully. They had no reason to believe that the information that they had relied on was obtained by or as a result of any breach of the Charter rights.

The Effect of the Breach on the Interests of the Accused

- [134] The accused argues that the warrantless search had a significant impact on the accused right to reasonable expectation of privacy. He argues that the whole purpose of the GigaTribe software was to exchange information so equitably and securely. I would add that it appears that the users also use it to exchange information anonymously. The accused does not make any claim that he was the person using the GigaTribe account. His only claim is in expectation of privacy and a hard drive that was connected to his computer and in his residence. The accused argues that the use of a network analyzer aggravated or created a greater intrusion on the reasonable expectation of privacy. I do not agree that added significantly to anything the police officer did. It was merely a tool which allowed him to obtain an IP address, which anybody could obtain, if they had access to the data. The network analyzing software also assisted in preserving the evidence which was contained in the files that were downloaded. The search was not intrusive when it was limited only to the files that Paper123boy had been offered to share. It did not include the search of a hard drive in a normal sense.
- [135] I agree with the Crown that the intrusion was fleeting and technical. The search of the residence was intrusive.
- [136] I also accept the Crown's argument that the recording of the information and the files was entirely consistent with Paper123boy's purpose in using the GigaTribe software, that is to share the files with others. He did not intend to share them with a police officer, but did intend to share them with anyone of his contacts that he sent the offer to.
- [137] The accused argued that the court should be concerned because the effect of admitting this evidence might be chilling on people who might want to use the GigaTribe software for some other purpose that was legitimate. However, I accept the Crown's argument that the only evidence before me is that the GigaTribe software appears to be used only for the purposes of exchanging child pornography or perhaps other forms of pornography. The evidence I have is from Detective Krawczyk who has investigated a large number of these

accounts and has found no other use. I do note however, that according to the GigaTribe website which was viewed in court, there are over 1.8 million users. I also note that Detective Krawczyk was not looking for other users who might have a legitimate purpose for using GigaTribe, but was looking for people who may be involved in internet exchange of child pornography.

[138] I also note Crown's argument that the extensive use of pseudonyms and the seeking of anonymity is not consistent with the type of legitimate uses that the accused speculated about, such as the use of this type of software by law firms or accountants or any other people who wish to exchange information in a secure way.

[139] I am not satisfied that the admission of this evidence would restrict the development or use of software that is designed for such purposes. I conclude that the admission of this evidence would do nothing to stop the development of other useful software that may be helpful to people intending to use the internet for legitimate purposes to safely and securely exchange information. It would be difficult for anybody today to be unaware, at least in a general sense, of the vast amount of software and programs available for parties to exchange information and data and the concerns for securing that from outside surveillance.

Society's Interest in an Adjudication on the Merits

[140] Both counsel agree that this evidence is central to the Crown's case. The accused argues however, that this must be considered in light of the seriousness of the breach and the individual interests at play. The accused also argues that although physical evidence is generally considered reliable, that there may be some questions raised about the reliability of the information on the 500 gigabyte hard drive which was not recovered on the first search. That hard drive was left in the apartment and not recovered until seven days later. We know that the landlord had access to that apartment during that time. The accused also refers to the fact that one group of the CD and DVDs appeared to have been lost during the investigation. The accused argues that these red flags should cause some concern about the handling of the evidence and the reliability of the physical evidence.

[141] The Crown responds by agreeing that the court must consider whether the true-seeking function of the criminal process would be better served by the admission of the evidence or by its exclusion. (Para. 79-86) This portion of the inquiry involves society's "collective interest in ensuring that those who transgress the law are brought to trial and dealt with according to the law". (Para 79)

[142] The Crown also points out in the words of Grant:

The admission of unreliable evidence serves neither the accused's interest in a fair trial nor the public interest in uncovering the truth. Conversely, exclusion of relevant and reliable evidence may undermine the truth-seeking function of the justice system and render the trial unfair from the public perspective, thus bringing the administration of justice into disrepute (paragraph 81)".

[143] I must consider the totality of the circumstances in making this analysis. The accused argues that "when the actions of Detective Krawczyk are considered through the eyes of an informed member of the public, the need for the exclusion of evidence becomes evident. The concern for having state agents intrude into the most private regions "cyber space" is real and disturbing. Failure to exclude the evidence would run the risk of condoning such interference".

[144] I disagree with the defence position. I am satisfied that a proper application of the Grant analysis supports the introduction of the evidence. To exclude the evidence in these circumstances would bring the administration of justice into disrepute.

[145] Therefore I dismiss the accused's application pursuant to s. 24(2) of the Charter.

Summary

[146] The accused applies to have evidence obtained as a result of the search of his residence excluded pursuant to s. 24(2) of the Charter on the basis that it infringed his right to be free from unreasonable search and seizure pursuant to s. 8 of the Charter.

[147] A search warrant was issued based on information obtained when Detective Krawczyk used a GigaTribe account with the username Devethedude2008. Detective Krawczyk obtained the password necessary to access this account when a man named Dan Quail was arrested in Tennessee. The police there searched his residence including his computer and provided the password to Detective Krawczyk. When Detective Krawczyk accessed the Devthedude2008 account, he could immediately see chat messages from a user under the name Paper123boy. He then accessed files that were being offered for sharing by Paper123boy. These files were on a hard drive which was attached to the accused's computer. Detective Krawczyk did not access any other portion of the accused's hard drive. Detective Krawczyk viewed and downloaded these files and while doing so, obtained the IP address attached to the downloads. He used that information to locate the internet service provider. He used a law enforcement request email to obtain the name and address of the account attached to the IP address at those particular times. He did this without a warrant. I am satisfied that this was not a warrantless search and was not an unreasonable search. A user in the GigaTribe account despite its use of "contacts" and encryption does not have a reasonable expectation of privacy in files offered for sharing or chats exchanged with that software. These chats and files are shared with other anonymous users and there is no evidence that those users have any idea who the other users are.

[148] The information obtained by Detective Krawczyk was properly used in the information to obtain and the search warrant properly issued. I have concluded that if there was a breach of s. 8, the exclusion of this evidence would bring the administration of justice into disrepute.

"R.E. Powers J."

POWERS J.

Source & reproduction note

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

ORIGINAL SOURCE <https://www.bccourts.ca/jdb-txt/SC/12/05/2012BCSC0525.htm>

CASE PAGE <https://chat.esheria.ai/case-law/canada/r-v-caza-2012>

Prepared on 29 October 2026 · Esheria