

**FEDERAL COURT**

**BETWEEN:**

**VOLTAGE PICTURES LLC**

**Plaintiff**

**and**

**JOHN DOE and JANE DOE**

**Defendants**

---

**MOTION RECORD OF THE PLAINTIFF,  
VOLTAGE PICTURES LLC**

*(Motion for a written examination of a non-party, returnable December 17, 2012)*

---

Date: December 11, 2012

**BRAUTI THORNINGZIBARRAS LLP**

151 Yonge Street, Suite 1800  
Toronto, ON M5C 2W7

**P. James Zibarras**  
**LSUC No. 48856F**

**John Philpott**  
**LSUC No. 60246U**

Tel.: 416.362.4567  
Fax: 416.362.8410

Lawyer for the Plaintiff,  
**VOLTAGE PICTURES LLC**

**TO:           TEKSAVVY SOLUTIONS INC.**  
C/O Stikeman Elliot LLP  
Suite 1600, 50 O'Connor Street  
Ottawa, ON K1P 6L2

**Nicholas McHaffie**

Tel:   613.566.0546

Lawyers for Responding Party,  
**TEKSAVVY SOLUTIONS INC.**

## INDEX

<u>TAB</u>		<u>PAGES</u>
<b>1</b>	<b>Notice of Motion, dated December 11, 2012</b>	<b>1-7</b>
<b>2</b>	<b>Affidavit of Barry Logan, sworn December 7, 2012</b>	<b>8-13</b>
A	Exhibit “A” - Voltage’s Cinematographic Works as Monitored by Canipre, from September 1, 2012 to October 31, 2012	14-16
B	Exhibit “B” - File Data, from September 1, 2012 to October 31, 2012	17-105
<b>3</b>	<b>Statement of Claim, issued on November 14, 2012</b>	<b>106-115</b>
<b>4</b>	<b>Memorandum of Fact and Law, dated December 11, 2012</b>	<b>116-139</b>
A	<i>BMG Canada Inc. v. Doe</i> , 2005 FCA 193	140-155
B	<i>Voltage Pictures LLC v. Jane Doe</i> , 2011 FC 1024	156-161
C	<i>R. v. Brzezinski</i> , 2009 CarswellOnt 8689	162-171
D	<i>R. v. Ward</i> , 2012 ONCA 660	172-191
E	<i>R v. Trapp</i> , 2011 SKCA 143	192-224

Court File No. T-2058-12

FEDERAL COURT

BETWEEN:

VOLTAGE PICTURES LLC

Plaintiff/Moving Party

and

JOHN DOE and JANE DOE

Defendants

---

**NOTICE OF MOTION**

*(Motion for a written examination of a non-party, returnable December 17, 2012)*

---

**TAKE NOTICE THAT** the Plaintiff, **VOLTAGE PICTURES LLC** (“Voltage”) will make a Motion to the Court on Monday, December 17, 2012, at 9:30 a.m., or as soon thereafter as the motion can be heard, at the Courthouse at 180 Queen Street West, Toronto, Ontario.

**PROPOSED METHOD OF HEARING:** The motion is to be heard orally.

**THE MOTION IS FOR:**

1. An Order pursuant to Rule 238 of the *Federal Court Rules* that TekSavvy Solutions Inc. (“TekSavvy”), a non-party to the action, be required to disclose to Voltage, in Microsoft Excel format, the contact information, including the names and addresses, of the TekSavvy customer accounts associated with the IP addresses attached as Exhibit “B” to the Affidavit of Barry Logan; and



2. Such further and other relief as counsel may advise and this Honourable Court may permit;

**THE GROUNDS FOR THE MOTION ARE:**

3. The Plaintiff, Voltage, is a movie production company based in Los Angeles, California. In 2012, Voltage retained Canipre Inc. (“Canipre”), a forensic investigation firm, to investigate whether Voltage’s cinematographic works (the “Works”) were being copied and distributed in Canada over peer to peer (“P2P”) networks using the BitTorrent Protocol;
4. The BitTorrent Protocol is a P2P file sharing protocol that facilitates the distribution of large amounts of data over the internet through networks. The BitTorrent Protocol breaks a file into numerous small data packets, allowing other network users or peers to download different sections of the same file from multiple users. This speeds up the time it takes to download a file and frees up the capacity of a computer or server to simultaneously download and upload files;
5. Once a packet is downloaded by a peer, that peer automatically becomes a download source for other peers connected to the Bit Torrent network who are requesting the file. Unless the settings on the user’s BitTorrent program are changed, every user who is copying or who has copied a file is simultaneously distributing it to every other user or peer connected to the BitTorrent network. This allows even small computers with low bandwidth to participate in large data transfers across a P2P network;

6. Between September 1 and October 30, 2012, Canipre used forensic software to scan BitTorrent networks for the presence of the Works. The forensic software searched BitTorrent networks for files corresponding to the Works and identified the IP address of each seeder or peer who was offering any of these files for transfer or distribution. This information is available to anyone that is connected to the P2P network;
7. The forensic software downloaded the copies of the Works available for distribution on the P2P networks and for each file downloaded recorded the following identifying information:
  - a. the IP address assigned to the peer by his or her internet service provider (“ISP”) at the time it distributed the file;
  - b. the date and time at which the file was distributed by the seeder or peer;
  - c. the P2P network utilized by the peer; and
  - d. the file’s metadata, which includes the name of the file and the size of the file (collectively, the “File Data”);
8. Canipre analyzed each of the BitTorrent packets distributed by the IP addresses contained in File Data and verified that reassembling the pieces results in a fully playable digital motion picture that is one of the Works. Canipre verified this by viewing a control copy of each of the Works side by side with the digital media files being distributed on the P2P network and confirming that they were the same;

9. Canipre reviewed the File Data and identified the transactions associated with IP addresses for customers of TekSavvy in Ontario that used the BitTorrent network to reproduce and distribute the Works during the period of September 1 to October 30, 2012 (the “Distributors”);
10. ISP’s track the IP addresses assigned to their customers at any given time and retain “user logs” of that information. Once provided with the IP address and the corresponding File Data, ISPs can review their user logs to identify the contact information of their clients who acted as peers to copy and distribute unauthorized versions of the Works. Only an ISP can correlate the IP address to the real identity of its subscriber;
11. In simple terms, the Distributors are facilitating the flagrant theft of the Works by others, on an international scale;
12. Voltage has a right to receive revenues, proceeds, and profits from its Works and has a proprietary interest in this right. Through their conduct, the Distributors have:
  - 1) contravened the *Copyright Act*;
  - 2) converted Voltage’s proprietary rights unto themselves;
  - 3) deprived Voltage of revenues and other consideration; and
  - 4) unlawfully interfered with Voltage’s economic relations;
13. All of the Distributors’ activities are done without the authorization of Voltage and without any payment or compensation to Voltage;

14. Voltage is therefore entitled to determine the identity of the Distributors and to pursue its available legal remedies against the Distributors, including an accounting and disgorgement of all revenues and profits (in whatever form) made by the Distributors from the wrongful conversion of Voltage's property, and damages from the losses of actual and prospective proceeds as a result of the Distributors' acts;
15. *Rules of Federal Court*, and in particular Rule 238;
16. Sections 27, 35, and 38.1 of *The Copyright Act*;
17. Such further and other grounds as counsel may advise and this Honourable Court may permit;

**THE FOLLOWING DOCUMENTARY EVIDENCE** will be relied on at the hearing of the motion:

18. The Affidavit of Barry Logan and the Exhibits thereto; and
19. Such further and other material as counsel may advise and this Honourable Court may permit.

December 11, 2012

**BRAUTI THORNING ZIBARRAS LLP**

151 Yonge Street, Suite 1800  
Toronto, ON M5C 2W7

P. James Zibarras  
LSUC No. 48856F

Tel: 416.362.4567  
Fax: 416.362.8410

Lawyers for the Plaintiff,  
**VOLTAGE PICTURES LLC**

**TO: TEKSAVVY SOLUTIONS INC.**  
C/O Stikeman Elliot LLP  
Attn: Nicholas McHaffie  
Suite 1600, 50 O'Connor Street  
Ottawa, ON K1P 6L2

Tel: 613-566-0546  
Email: [nmchaffie@stikeman.com](mailto:nmchaffie@stikeman.com)

Lawyers for Responding Party,  
**TEKSAVVY SOLUTIONS INC**

**VOLTAGE PICTURES LLC**  
Plaintiff/Moving Party

and

**JOHN DOE and JANE DOE**  
Defendants

**FEDERAL COURT**

Proceeding commenced at Toronto

**NOTICE OF MOTION**

*(Motion for a written examination of a non-party,  
returnable December 17, 2012)*

**BRAUTI THORNING ZIBARRAS LLP**

151 Yonge Street, Suite 1800  
Toronto, ON M5C 2W7

**P. James Zibarras**  
**LSUC No. 48856F**

**John Philpott**  
**LSUC No. 60246U**

**Tel: 416.362.4567**  
**Fax: 416.362.8410**

**Lawyers for the Plaintiff,  
VOLTAGE PICTURES LLC**

**Court File No. CV-**

**FEDERAL COURT**

**BETWEEN:**

**VOLTAGE PICTURES LLC**

Plaintiff

**and**

**JOHN DOE and JANE DOE**

Defendants

**AFFIDAVIT OF BARRY LOGAN**

(Sworn on December 7, 2012)

I, **BARRY LOGAN**, of the City of Stratford, in the province of Ontario, **MAKE OATH AND SAY AS FOLLOWS:**

1. I am the owner and principal forensic consultant of Canipre Inc. ("Canipre"), an Ontario based corporation that provides forensic investigation services to copyright owners. As part of my duties at Canipre, I routinely identify the Internet Protocol ("IP") addresses used by individuals who download and distribute copyrighted works over peer to peer ("P2P") networks using the BitTorrent Protocol.

2. The Plaintiff, Voltage Pictures LLC ("Voltage"), is a movie production company based in Los Angeles, California. Voltage retained Canipre to investigate whether its films were being copied and distributed by Canadian members of P2P online networks and to support the associated litigation. I was directly involved in the investigation and as such

have knowledge of the matters to which I hereinafter depose. Where I do not have personal knowledge, I have stated the source of my information and believe it to be true.

***Background – The BitTorrent Protocol***

3. The BitTorrent Protocol is a P2P file sharing protocol that facilitates the distribution of large amounts of data over the internet through networks.

4. When a file is initially uploaded to a BitTorrent network, that is referred to as “seeding”. Other P2P networks users, called “peers”, can then connect to the user seeding the file in order to copy it.

5. The BitTorrent Protocol breaks a file into numerous small data packets, each of which is identifiable by a unique hash number created using a hash algorithm. Once a file has been broken into numerous packets, other network users or peers are able to download different sections of the same file from multiple users. Each new peer is directed to the most readily available packet of the file they wish to download. In other words, a peer does not copy a file from one user, but from any peer who previously downloaded the file and has it available on the BitTorrent network. The peer then becomes a seeder as it distributes the data packet to other peers connected to the BitTorrent network.

6. Once a packet is downloaded by a peer, that peer automatically becomes a download source for other peers connected to the BitTorrent network who are requesting the file. This speeds up the time it takes to download a file and frees up the capacity of a computer or server to simultaneously download and upload files. Unless the settings on the user’s BitTorrent program are changed, every user who is copying or who has copied a file is



simultaneously distributing it to every other user or peer connected to the BitTorrent network. This allows even small computers with low bandwidth to participate in large data transfers across a P2P network.

***Canipre's Forensic Investigation***

7. Voltage retained Canipre to identify the Internet Protocol ("IP") addresses used on the BitTorrent network to copy and distribute copyrighted works which Voltage has the rights to in Canada. A list of such works which Canipre monitored as part of this investigation is attached as **Exhibit "A"**.

8. Between September 1 and October 31, 2012, forensic software called GuardaLey Observer v1.2 (the "Forensic Software") was used to scan BitTorrent networks for the presence of Voltage's copyrighted works.

9. I was tasked with monitoring, analyzing, reviewing and attesting to the results of the investigation.

10. The Forensic Software was run between September 1 and October 31, 2012. The Forensic Software searched BitTorrent networks for files corresponding to Voltage's copyrighted works and identified the IP address of each seeder or peer who was offering any of these files for transfer or distribution. This information is available to anyone that is connected to the P2P network.

11. The Forensic Software then downloaded the copies of Voltage's copyrighted works available for distribution on the P2P networks, and for each file downloaded recorded the following identifying information:

- a. the IP address assigned to the peer by his or her internet service provider (“ISP”) at the time it distributed the file;
- b. the date and time at which the file was distributed by the seeder or peer;
- c. the P2P network utilized by the peer; and
- d. the file’s metadata, which includes the name of the file and the size of the file (collectively, the “File Data”).

12. The File Data is stored in a secure central database. I have personally reviewed the File Data. After reviewing the File Data, I identified the transactions associated with IP addresses geographically limited to Ontario and to customers of TekSavvy Solutions Inc. (“TekSavvy”) that used the BitTorrent network to reproduce and distribute Voltage’s copyrighted works during the period of September 1 to October 31, 2012. A copy of the File Data for these transactions is attached as **Exhibit “B”**.

### *Identifying the IP Addresses*

13. An internet service provider or ISP, such as TekSavvy, is an organization which provides access to the Internet to its customers. Peers, seeds, and users access the BitTorrent network through the internet access provided by their ISP.

14. An IP address is a unique numerical identifier that is automatically assigned to an internet user by that user’s ISP.

15. ISPs are assigned blocks or ranges of IP addresses. The range assigned to any ISP can be found in publicly available databases on the internet.

16. ISPs track the IP addresses assigned to their customers at any given time and retain “user logs” of that information.

17. Through the Forensic Software, I am able to track a peer by its IP address to a particular ISP and to their geographic location. This is how I was able to limit the IP addresses and related File Data in Exhibit B to customers of TekSavvy in the province of Ontario.

18. Once provided with the IP address and the corresponding File Data, ISPs can review their user logs to identify the name, address, email address, and phone number of their clients who acted as peers to copy and distribute unauthorized versions of Voltage’s works.

19. Only an ISP can correlate the IP address to the real identity of its subscriber. Without the involvement of the ISPs, Voltage will be unable to determine the identities of those persons who are distributing their copyrighted works.

### ***Confirmation of Data***

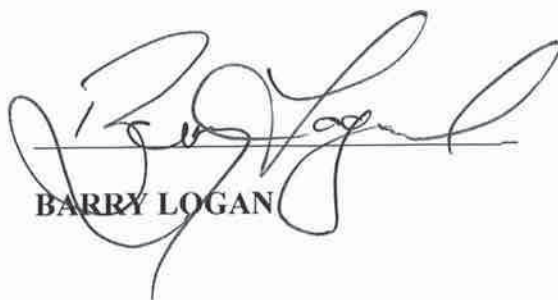
20. I personally reviewed the File Data gathered from this investigation.

21. After reviewing the File Data, I verified that the transactions contained in Exhibit B are associated with IP addresses geographically limited to Ontario and to customers of TekSavvy. I have also verified that the IP addresses and related File Data contained in Exhibit B hereto correctly reflect what is contained in the secure central databases.

22. In addition, I have analyzed each of the BitTorrent packets distributed by the IP addresses listed in Exhibit B and verified that reassembling the pieces results in a fully playable digital motion picture that is one of Voltage's copyrighted works.

23. I was provided with a control copy of each of Voltage's copyrighted works, which I have viewed side by side with the digital media files set forth in Exhibit B and confirmed that they were the same.

SWORN BEFORE ME at the City of )  
 Toronto, in the Province of Ontario, )  
 this 1 day of December, 2012 )  
 \_\_\_\_\_ )  
 \_\_\_\_\_ )  
 A Commissioner of Oaths, etc.

BARRY LOGAN

Nanci Elizabeth McFadden-Fair,  
 a Commissioner, etc., Province of Ontario,  
 for Michael F. Fair, Barrister and Solicitor.  
 Expires November 26, 2015.

**VOLTAGE PICTURES LLC**  
Plaintiff

and

**JOHN DOE and JANE DOE**  
Defendants

**ONTARIO  
SUPERIOR COURT OF JUSTICE**

Proceeding commenced at Toronto

**AFFIDAVIT OF BARRY LOGAN**  
(Sworn on December 2012)

**BRAUTI THORNING ZIBARRAS LLP**  
151 Yonge Street, Suite 1800  
Toronto, ON M5C 2W7


**P. James Zibarras**  
**LSUC No. 48856F**

**John Philpott**  
**LSUC No. 60246U**

Tel: 416.362.4567  
Fax: 416.362.8410

**Lawyers for the Plaintiff,  
VOLTAGE PICTURES LLC**

This is **Exhibit "A"** referred to in the  
affidavit of **BARRY LOGAN** sworn before me  
this 7 day of December, 2012.



---

A COMMISSIONER FOR TAKING AFFIDAVITS

Nanci Elizabeth McFadden-Fair,  
a Commissioner, etc., Province of Ontario,  
for Michael F. Fair, Barrister and Solicitor.  
Expires November 26, 2015.

**Voltage's Cinematographic Works as Monitored by Canipre**

**09.01.12 – 10.31.12**

Generation Um ... (2012)

Tucker & Dale vs Evil (2010)

True Justice (The Complete First Season) (2010)

The Third Act aka The Magic of Belle Isle (2012)

The Good Doctor (2011)

Rosewood Lane (2011)

Another Happy Day aka The Reasonable Bunch (2011)

Killer Joe (2011)

Escapee (2011)

This is **Exhibit "B"** referred to in the  
affidavit of **BARRY LOGAN** sworn before me  
this     day of December, 2012.



---

*A COMMISSIONER FOR TAKING AFFIDAVITS*

**Nanci Elizabeth McFadden-Fair,**  
**a Commissioner, etc., Province of Ontario,**  
**for Michael F. Fair, Barrister and Solicitor.**  
**Expires November 26, 2015.**





Court File No.

34  
T-2058-12

**FEDERAL COURT**

**VOLTAGE PICTURES LLC**

**Plaintiff**

**-and-**

**JOHN DOE AND JANE DOE**

**Defendants**

---

**STATEMENT OF CLAIM**

---

TO THE DEFENDANTS:

A LEGAL PROCEEDING HAS BEEN COMMENCED AGAINST YOU by the Plaintiff. The claim made against you is set out in the following pages.

IF YOU WISH TO DEFEND THIS PROCEEDING, you or a solicitor acting for you are required to prepare a statement of defence in Form 171B prescribed by the *Federal Courts Rules*, serve it on the plaintiff's solicitor or, where the plaintiff does not have a solicitor, serve it on the plaintiff, and file it, with proof of service, at a local office of this Court, WITHIN 30 DAYS after this statement of claim is served on you, if you are served within Canada.

If you are served in the United States of America, the period for serving and filing your statement of defence is forty days. If you are served outside Canada and the United States of America, the period for serving and filing your statement of defence is sixty days.

Copies of the *Federal Courts Rules*, information concerning the local offices of the Court and other necessary information may be obtained on request to the Administrator of this Court at Ottawa (telephone 613-991-4238) or at any local office.

IF YOU FAIL TO DEFEND THIS PROCEEDING, judgment may be given against you in your absence and without further notice to you.

**TORONTO**, this 14<sup>th</sup> day of November, 2012

Issued by:



**CHARLES SKELTON**  
**REGISTRY OFFICER**  
**AGENT DU GREFFE**

Address of local office:  
Federal Court of Canada  
180 Queen Street West  
Toronto, ON M5V 3L6

Tel.: (416) 973-3356  
Fax.: (416) 954-5068

Defendants: **John Doe and Jane Doe**  
Addresses Unknown

**CLAIM**

1. The Plaintiff, Voltage Pictures LLC (“Voltage”), claims against John Doe, Jane Doe and other persons unknown (collectively, the “Defendants”) for:

- a) a declaration that the Defendants’ unauthorized reproduction and distribution of the Plaintiff’s copyrighted cinematographic works, listed in Schedule “A” (the “Works”), constitutes an infringement of the Plaintiff’s rights contrary to sections 27(1) and 27(2) of the *Copyright Act*;
- b) an interim, interlocutory and permanent injunction restraining each Defendant, and any and all persons acting on behalf of or in conjunction with any of them or any and all persons with notice of this injunction, from downloading, reproducing, and distributing the Works;
- c) statutory damages pursuant to s. 38.1 of the *Copyright Act*;
- d) in the alternative, actual damages pursuant to s. 35 of the *Copyright Act* in an amount to be proven at trial;
- e) an accounting of all profits from the Defendants’ wrongful activities;
- f) damages for conversion, unlawful interference with economic relations and unjust enrichment in an amount to be proven at trial;
- g) aggravated, exemplary and punitive damages in the amount of \$10,000.00;
- h) special damages, the particulars of which will be provided prior to trial;

- i) pre-judgment and post-judgment interest pursuant to ss. 36 and 37 *Federal Court Act*, R.S.C. 1985, c. F-7, as amended;
- j) costs of this action on a substantial indemnity basis, plus applicable taxes; and
- k) such further and other relief as this Honourable Court may deem just.

### **The Parties**

2. The Plaintiff, Voltage Pictures LLC (“Voltage”), is a movie production company based in Los Angeles, California, with exclusive rights to lawfully distribute the Works in Canada.

3. The Defendants are persons whose names and identities are currently unknown to the Plaintiff, but who have unlawfully and without Voltage’s authorization or consent copied and distributed Voltage’s protected Works in breach of the laws of Canada.

### **The Unauthorized Distribution of the Works Through the BitTorrent Protocol**

4. The Defendants are members of peer-to-peer (“P2P”) internet networks that have used the BitTorrent Protocol to copy and distribute the Works without authorization.

5. The BitTorrent Protocol is a P2P file sharing protocol that facilitates the distribution of large amounts of data over the internet through networks.

6. When a file is initially uploaded to a P2P network, that is referred to as “seeding”. Other P2P networks users, called “peers”, can then connect to the user seeding the file in order to copy it.

7. The BitTorrent Protocol breaks a file into numerous small data packets, each of which is identifiable by a unique hash number created using a hash algorithm. Once a file has been broken into numerous packets, other network users or peers are able to download different sections of the same file from multiple users. Each new peer is directed to the most readily available packet of the file they wish to download. In other words, a peer does not copy a file from one user, but from any peer who previously downloaded the file and has it available on the BitTorrent network. The peer then becomes a seeder as it distributes the data packet to other peers connected to the BitTorrent network.

8. Once a packet is downloaded by a peer, that peer automatically becomes a download source for other peers connected to the Bit Torrent network who are requesting the file. This speeds up the time it takes to download a file and frees up the capacity of a computer or server to simultaneously download and upload files. Unless the settings on the user's BitTorrent program are changed, every user who is copying or who has copied a file is simultaneously distributing it to every other user or peer connected to the BitTorrent network. This allows even small computers with low bandwidth to participate in large data transfers across a P2P network.

### **The Actions of the Defendants**

9. Through a forensic investigation, the Plaintiff has identified the Defendants (identified by their Internet Protocol ("IP") addresses), as having participated through P2P networks in the unauthorised copying and distribution of Voltage's Works. An IP address is a unique numerical identifier assigned to an internet user by that user's internet

service provider (“ISP”). Once the Plaintiff obtains the Defendants’ contact information from their ISPs, it will be able to name those Defendants as parties to this claim.

10. In simple terms, the Defendants are engaging in the flagrant theft of Voltage’s works and, in addition, are intentionally facilitating and assisting in the theft of those same Works by others, on an international scale.

11. Voltage has a right to receive revenues, proceeds, and profits from its Works and has a proprietary interest in this right. Through their conduct, the Defendants have:

- a) contravened the *Copyright Act*;
- b) converted Voltage’s proprietary rights unto themselves;
- c) deprived Voltage of revenues and other consideration; and
- d) unlawfully interfered with Voltage’s economic relations.

12. All of the Defendants’ activities are done without the authorization of Voltage and without any payment or compensation to Voltage.

13. Voltage is therefore entitled to an accounting and disgorgement of all revenues and profits (in whatever form) made by the Defendants from the wrongful conversion of Voltage’s property, and damages from the losses of actual and prospective proceeds as a result of the Defendants’ acts.

14. By trafficking in, offering and distributing the Works, the Defendants have directly and intentionally facilitated the unauthorized reception, distribution and use of Voltage’s protected works by persons not authorized to receive them. The Defendants

have thereby unlawfully interfered with Voltage's economic relations with its customers and lawful distributors, and are liable therefor.

15. By reason of the foregoing, the Defendants are liable for all pecuniary losses suffered by Voltage as a result of their interference.

16. Voltage generates its revenues through the lawful distribution and sales of its works. It is critical to Voltage that access to its Works be conditional on payment of a purchase price. The sole purpose of the Defendants' P2P activities, apart from commercial gain, is to permit consumers to receive and view Voltage's Works without payment to Voltage and without charge. The Defendants' activities are carried out intentionally, with full knowledge of Voltage's rights, and without Voltage's consent. As a direct and proximate result of their wrongful acts, the Defendants have been unjustly enriched and Voltage has suffered, and will continue to suffer, loss of revenues, proceeds and profits. The exact amount of unjust profits realized by the Defendants and profits lost by Voltage are presently unknown and cannot be readily ascertained without an accounting.

### **Damages**

17. The Plaintiff claims statutory damages pursuant to s. 38.1 of the *Copyright Act*.

18. Alternatively, the Plaintiff claims damages pursuant to s. 35 of the *Copyright Act* in an amount to be proven at trial.

19. Voltage sustains an economic loss every time the Defendants use P2P networks to make the Works available to be received and viewed. As a result of the Defendants'


conduct in copying and distributing the Works, Voltage has suffered and continues to suffer loss, damage and expense, in an amount to be proved at trial, while the Defendants have benefited and profited and continue to benefit and profit from their wrongful activities.

20. The Defendants have acted in a high-handed, malicious, and reprehensible fashion, and in wanton and reckless disregard for Voltage's rights, which ought not to be countenanced by this Honourable Court. Accordingly, Voltage is entitled to punitive, aggravated, and exemplary damages.

21. The Plaintiff proposes this action be tried in Toronto, Ontario.

DATED AT TORONTO, this 14<sup>th</sup> day of November, 2012.

**BRAUTI THORNING ZIBARRAS LLP**

Per:  P. James Zibarras

**BRAUTI THORNING ZIBARRAS LLP**

151 Young Street, Suite 1800  
Toronto, ON M5C 2W7

**James Zibarras**  
**LSUC No. 48856F**  
**jzibarras@btzlaw.ca**

**John Philpott**  
**LSUC No. 60246U**  
**jphilpott@btzlaw.ca**

Tel.: 416.362.4567  
Fax: 416.362.8410

Lawyers for the Plaintiff,  
**VOLTAGE PICTURES LLC**



**SCHEDULE "A"****Voltage's Cinematographic Works**

Generation Um ... (2012)  
Tucker & Dale vs Evil (2010)  
The Whistleblower (2010)  
True Justice: Brotherhood (2010)  
The Third Act aka The Magic of Belle Isle (2012)  
Breathless (2012)  
Peace Love & Misunderstanding (2011)  
Conviction (2010)  
The Good Doctor (2011)  
Faces in the Crowd (2011)  
Rosewood Lane (2011)  
Puncture (2011)  
Another Happy Day aka Reasonable Bunch (2011)  
The Barrens (2012)  
True Justice: Lethal Justice (2010)  
True Justice: Blood Alley (2010)  
Killer Joe (2011)  
Maximum Conviction (2012)  
Fire with Fire (2012)  
Rites of Passage (2012)  
True Justice: Urban Warfare (2010)  
True Justice: Deadly Crossing (2010)  
Rites of Passage AKA Party Killers (2012)  
Balls to the Wall (2011)  
Sacrifice (2011)  
Escapee (2011)  
True Justice: Dark Vengeance (2010)

**VOLTAGE PICTURES LLC**  
Plaintiff

and

**JOHN DOE and JANE DOE**  
Defendants

**FEDERAL COURT**

Proceeding commenced at Toronto

**STATEMENT OF CLAIM**

**BRAUTI THORNING ZIBARRAS LLP**  
151 Yonge Street, Suite 1800  
Toronto, ON M5C 2W7

**P. James Zibarras**  
**LSUC No. 48856F**  
**jzibarras@btzlaw.ca**

**John Philpott**  
**LSUC No. 60246U**  
**jphilpott@btzlaw.ca**

**Tel: 416.362.4567**  
**Fax: 416.362.8410**

Lawyers for the Plaintiff,  
**VOLTAGE PICTURES LLC**

Court File No.: T-2058-12

FEDERAL COURT

B E T W E E N:

VOLTAGE PICTURES LLC

Plaintiff

and

JOHN DOE and JANE DOE

Defendants

MOTION UNDER RULE 238 of the FEDERAL COURT RULES, 1998 (SOR/98-106), as amended.

---

MEMORANDUM OF FACT AND LAW

---

Date: December 11, 2012

**BRAUTI THORNING ZIBARRAS LLP**  
151 Yonge Street, Suite 1800  
Toronto, ON M5C 2W7

**James Zibarras**  
**LSUC No. 48856F**

**John Philpott**  
**LSUC No. 60246U**

Tel.: 416.362.4567  
Fax: 416.362.8410

Lawyers for the Plaintiff,  
**VOLTAGE PICTURES LLC**

**TO: TEKSAVVY SOLUTIONS INC.**

C/O Stikeman Elliot LLP

Attn: Nicholas McHaffie

Suite 1600, 50 O'Connor Street

Ottawa, ON K1P 6L2

Tel: 613-566-0546

Email: [nmchaffie@stikeman.com](mailto:nmchaffie@stikeman.com)

Lawyers for Responding Party,

**TEKSAVVY SOLUTIONS INC.**

## TABLE OF CONTENTS

<b>PART I – OVERVIEW .....</b>	<b>1</b>
<b>PART II – STATEMENT OF FACTS.....</b>	<b>1</b>
The Parties .....	1
The BitTorrent Protocol.....	2
The Plaintiff’s Forensic Investigation.....	3
Identifying the IP Addresses.....	4
<b>PART III – POINTS IN ISSUE.....</b>	<b>5</b>
<b>PART IV – SUBMISSIONS.....</b>	<b>6</b>
The Test for Granting Leave to Examine a Non-Party .....	6
Voltage has a Bona Fide Claim .....	7
TekSavvy is the Only Source of the Relevant Information .....	7
An Order is the Only Reasonable Method of Obtaining this Information.....	8
Fairness dictates that Voltage should Receive the Information.....	8
An Order is the Only Reasonable Method of Obtaining this Information.....	9
Privacy Concerns .....	10
<b>PART V – ORDER SOUGHT .....</b>	<b>11</b>
<b>PART VI – LIST OF AUTHORITIES .....</b>	<b>11</b>
<b>APPENDIX “A” – STATUTES AND REGULATIONS.....</b>	<b>13</b>

## **PART I - OVERVIEW**

1. This is a motion made by the Plaintiff, Voltage Pictures LLC (“Voltage”), for an Order pursuant to Rule 238 of the *Federal Court Rules* and the principles of equitable discovery, compelling Teksavvy Solutions Inc. (“Teksavvy”), a non-party Internet Service Provider (“ISP”), to disclose the contact information of their subscribers involved in the unauthorized copying and distribution of Voltage’s copyrighted cinematographic works, listed in Exhibit “A” to the Affidavit of Barry Logan (the “Works”).

## **PART II – STATEMENT OF FACTS**

### **(i) The Parties**

2. Voltage is well known and highly regarded film production company based in Los Angeles, California. Voltage has exclusive rights to lawfully distribute its copyrighted cinematographic Works.

**Affidavit of Barry Logan, sworn December 7, 2012 at Tab 2 of the Motion Record (“Logan Affidavit”) at paras. 2 & 7**

3. The Defendants are persons whose names and identities are currently unknown to the Plaintiff, but who have unlawfully and without Voltage’s authorization or consent copied and distributed Voltage’s protected Works through peer to peer (“P2P”) internet networks using the BitTorrent Protocol, in breach of the laws of Canada.

**Statement of Claim, at Tab 3 of the Motion Record (the “Statement of Claim”) at para. 3**

4. The non-party, Teksavvy, is an ISP based in Canada. ISPs, such as Teksavvy, are organizations which provide their customers with access to the Internet.

**Logan Affidavit at para. 13**

5. The Plaintiff requires Teksavvy to disclose the contact information of their subscribers, listed in Exhibit B to the Affidavit of Barry Logan, who have unlawfully copied and distributed Voltage's copyrighted Works over the Internet, so that they can be named in the within litigation.

**Logan Affidavit at para. 19; Statement of Claim**

**(ii) The BitTorrent Protocol**

6. The BitTorrent Protocol is a P2P file sharing protocol that facilitates the distribution of large amounts of data over the internet through networks.

**Logan Affidavit at para. 3**

7. When a file is initially uploaded to a BitTorrent network, that is referred to as "seeding". Other P2P networks users, called "peers", can then connect to the user seeding the file in order to copy it.

**Logan Affidavit at para. 4**

8. The BitTorrent Protocol breaks a file into numerous small data packets, each of which is identifiable by a unique hash number created using a hash algorithm. Once a file has been broken into numerous packets, other network users or peers are able to download different sections of the same file from multiple users. Each new peer is directed to the most readily available packet of the file they wish to download. In other words, a peer does not copy a file from one user, but from any peer who previously downloaded the file and has it available on the BitTorrent network. The peer then becomes a seeder as it distributes the data packet to other peers connected to the BitTorrent network.

**Logan Affidavit at para. 5**

9. Once a packet is downloaded by a peer, that peer automatically becomes a download source for other peers connected to the BitTorrent network who are requesting the file. This speeds up the time it takes to download a file and frees up the capacity of a computer or server to simultaneously download and upload files. Unless the settings on the user's BitTorrent program are changed, every user who is copying or who has copied a file is simultaneously distributing it to every other user or peer connected to the BitTorrent network. This allows even small computers with low bandwidth to participate in large data transfers across a P2P network.

**Logan Affidavit at para. 6**

**(iii) The Plaintiff's Forensic Investigation**

10. Between September 1 and October 31, 2012, the Plaintiff requisitioned a forensic investigation using forensic software called GuardaLey Observer v1.2 (the "Forensic Software") to scan BitTorrent networks for the presence of Voltage's copyrighted Works.

**Logan Affidavit at para. 8**

11. The Forensic Software searched BitTorrent networks for files corresponding to Voltage's copyrighted Works and identified the IP address of each seeder or peer who was offering any of these files for transfer or distribution. This information is available to anyone that is connected to the P2P network.

**Logan Affidavit at para. 10**

12. The Forensic Software then downloaded the copies of Voltage's copyrighted Works available for distribution on the P2P networks and for each file downloaded recorded the following identifying information:



- a) the IP address assigned to the peer by his or her internet service provider (“ISP”) at the time it distributed the file;
- b) the date and time at which the file was distributed by the seeder or peer;
- c) the P2P network utilized by the peer; and
- d) the file’s metadata, which includes the name of the file and the size of the file (collectively, the “File Data”).

**Logan Affidavit at para. 11**

13. The File Data is stored in a secure central database. The Plaintiff’s forensic consultants reviewed the File Data and isolated the transactions associated with IP addresses geographically limited to Ontario and to customers of Teksavvy that used the BitTorrent network to reproduce and distribute Voltage’s copyrighted works during the period of September 1 to October 15, 2012.

**Logan Affidavit at para. 12**

**(iv) Identifying the IP Addresses**

14. Through its forensic investigation, the plaintiff, Voltage, has identified the IP addresses listed as Exhibit B to the Affidavit of Barry Logan as having participated through P2P networks in the unauthorised copying and distribution of Voltage’s Works.

**Logan Affidavit, see paras. 7-12 & 20-23**

15. At this time, each of the Defendants has been identified only by the unique IP address assigned to it by that user’s ISP.

**Logan Affidavit at para. 7-12 & 14-15 & 17**

16. ISPs track the IP addresses assigned to their customers at any given time and retain “user logs” of that information.

**Logan Affidavit at para. 16**

17. Once provided with the IP address and the corresponding File Data, ISPs can review their user logs to identify the name, address, email address, and phone number of their clients who acted as peers to copy and distribute unauthorized versions of Voltage’s works.

**Logan Affidavit at para. 18**

18. Only an ISP can correlate the IP address to the real identity of its subscriber. Without the involvement of the ISPs, Voltage will be unable to determine the identities of those persons who are distributing their copyrighted works.

**Logan Affidavit at para. 19**

19. Once the Plaintiff obtains the Defendants’ contact information from their ISPs, it will be able to name those Defendants as parties to this claim.

**Logan Affidavit at para. 2; Statement of Claim**

### **PART III – POINTS IN ISSUE**

20. It is respectfully submitted that the sole issue on this Motion is whether Voltage should be granted leave to conduct a written examination of Teksavvy for the sole purpose of obtaining the contact information of potential defendants to this action?

#### **PART IV – SUBMISSIONS**

21. In copyright infringement cases, Courts will order non-parties to disclose the contact information of potential defendants where plaintiffs have a *bona fide* claim against unknown infringers. As Justice Sexton states in the leading Federal Court of Appeal decision of *BMG Canada Inc. v. Doe*, “Thus, in my view, in cases where plaintiffs show that they have a *bona fide* claim that unknown persons are infringing their copyright, they have a right to have the identity revealed for the purposes of bringing an action.”

*BMG Canada Inc. v. Doe*, 2005 FCA 193 (“*BMG*”) per Sexton J. at paras. 42

**(i) The Test for Granting Leave to Examine a Non-Party**

22. Following *BMG*, the Plaintiff’s right to know the identity of potential defendants stems from Rule 238 of the *Federal Court Rules* and the principles of equitable bills of discovery. Accordingly, the Plaintiff will be entitled to a written examination of TekSavvy if:

- a) the Plaintiff has a *bona fide* case;
- b) the non-party, TekSavvy, has information on an issue in the action;
- c) an order is the only reasonable means of obtaining the information;
- d) it is fair to require that the information be provided prior to trial; and
- e) an order will not cause undue delay, inconvenience or expense to TekSavvy or other parties.

*BMG Canada Inc. v. Doe*, 2005 FCA 193 (“*BMG*”) per Sexton J. at paras. 23-35; *Voltage Pictures LLC v. Jane Doe*, 2011 FC 1024 (“*Voltage*” at para. 16); Rule 238 of the *Federal Court Rules*, SOR/98-106

23. Each of these criteria will be discussed in turn below.

**(a) Voltage has a Bona Fide Claim**

24. Voltage has satisfied the low threshold of demonstrating a *bona fide* claim. As indicated by the Federal Court of Appeal in *BMG*, a *bona fide* claim is a lower threshold than demonstrating a *prima facie* case. As Justice Sexton states,

In my view, it would make little sense to require proof of a *prima facie* case at the stage of the present proceeding. The plaintiffs do not know the identity of the persons they wish to sue, let alone the details of precisely what was done by each of them such as to actually prove infringement. Such facts would only be established after examination for discovery and trial. *The plaintiffs would be effectively stripped of a remedy if the courts were to impose upon them, at this stage, the burden of showing a prima facie case. It is sufficient if they show a bona fide claim, i.e. that they really do intend to bring an action for infringement of copyright based upon the information they obtain, and that there is no other improper purpose for seeking the identity of these persons.*

*BMG, supra*, at para. 34 (*emphasis added*)

25. Voltage's intent to bring an action for copyright infringement is established by Voltage's Statement of Claim filed in the within action. In addition, Voltage has to date retained a forensic investigative firm to identify the relevant IP addresses and provide support during the litigation, and retained legal counsel to prepare, file and pursue the Statement of Claim against the unnamed Defendants which it seeks to identify through the within motion.

Logan Affidavit at para. 2; Statement of Claim; Notice of Motion at Tab 1 of the Motion Record

**(ii) TekSavvy is the Only Source of the Relevant Information**

26. TekSavvy is the only available source of the contact information that corresponds with the IP addresses which have been identified as copying and distributing Voltage's works.

s. 238(a), *Federal Court Rules*; Logan Affidavit at paras. 13-19

27. The contact information of the individuals who have been copying and distributing Voltage's Works is clearly relevant to Voltage's proposed action, as it is the only method of identifying the John and Jane Doe defendants.

*Voltage, supra*, at para. 21; Logan Affidavit at para. 13-19

**(iii) An Order is the Only Reasonable Method of Obtaining this Information**

28. Under the extant privacy legislation, the ISPs require an Order of this Court to disclose the requested information. Therefore, an Order is the only method of acquiring the needed information.

*s. 7(3)(c), Personal Information Protection and Electronic Documents Act, SC 2000, c 5; Voltage, supra*, at para. 22; *BMG, supra*, at para. 37; *s. 238(b), Federal Court Rules*

29. Voltage is only able to obtain this information by means of an Order. As stated above, the information sought is solely within the ISPs possession. In essence, without obtaining documentary disclosure from the ISP, Voltage will be prevented from protecting its rights.

**(iv) Fairness dictates that Voltage should Receive the Information**

30. Voltage's ability to protect its rights hinges on obtaining the Order sought herein. The Federal Court of Appeal has confirmed that, upon demonstrating a *bona fide* claim, rights holders are entitled to have the identity of the alleged infringer revealed by the ISP.

*s. 238(c), Federal Court Rules; BMG, supra*, at para. 42, quoted approvingly in *Voltage, supra*, at para. 23

31. As stated by Justice Shore in *Voltage*, “Defendants should not have the possibility of hiding behind the anonymity of the internet and continuing to infringe the copyright of Voltage Pictures LLC.”

*Supra*, at para. 25

32. As Voltage should be allowed to protect its rights, fairness requires that Voltage should be allowed to obtain disclosure from the ISPs.

**(v) The Order will not cause Undue Delay, Inconvenience or Expense**

33. The Order will not cause undue delay, inconvenience, or expense to TekSavvy or to other parties (as they are currently unknown). In contrast, without obtaining this information, the results of Voltage’s forensic investigation will become stale, Voltage’s ability to pursue the Defendants will be indefinitely delayed and its rights will remain compromised.

**s. 238(d), Federal Court Rules**

34. Importantly, ISPs have the requested information at their fingertips. Identifying and dealing with their own customers is at the core of their business and engaged in daily. Furthermore, ISP’s are already staffed and equipped to provide such information to third parties, as they do so regularly in criminal matters. This is in effect part of their business and their systems are set up to make the retrieval of such information quick and easy. For example, in *R. v. Brzezinski*, an ISP was able to determine the contact information associated with an IP address on the same day the request was made.

E.g., see *R. v. Brzezinski*, 2009 CarswellOnt 8689, per A.W. Bryant J. at para. 8-10; see also *R. v. Ward*, 2012 ONCA 660 per Doherty J.A. at paras. 2-3.

35. Also, Voltage has undertaken to reimburse any reasonable expenses incurred by TekSavvy in providing the information.

**(vi) Privacy Concerns**

36. In *BMG*, the Federal Court of Appeal considered the privacy concerns at issue on motions such as this and held as follows:

Modern technology such as the Internet has provided extraordinary benefits for society, which include faster and more efficient means of communication to wider audiences. This technology must not be allowed to obliterate those personal property rights which society has deemed important. Although privacy concerns must also be considered, it seems to me that they must yield to public concerns for the protection of intellectual property rights in situations where infringement threatens to erode those rights. Thus, in my view, in cases where plaintiffs show that they have a *bona fide* claim that unknown persons are infringing their copyright, they have a right to have the identity revealed for the purpose of bringing an action.

*Supra*, at para. 41-42

37. In the criminal context, both the Saskatchewan Court of Appeal and the Ontario Court of Appeal have determined that there is no reasonable expectation of privacy for an ISP to withhold the personal contact information associated with an IP address.

*R v. Trapp*, 2011 SKCA 143 per Cameron J.A.; *R. v. Ward*, 2012 ONCA 660 per Doherty J.A

38. It should not be ignored that when individuals use P2P networks, they publicly reveal their IP address and which files they are copying and distributing. As stated by the Saskatchewan Court of Appeal, an individual puts “into the public realm, on the Gnutella network [a P2P network], information about his activities or lifestyle...”. In addition, as noted by the Court of Appeal, contact information is generally available in public directories, which weighs against there being an expectation of privacy in it.

Logan Affidavit at para. 10; *R v. Trapp*, *supra*, at paras. 134-135

39. The jurisprudence in the copyright context as well as the criminal context reflects the reality that individuals who infringe on the rights of others should not be allowed to hide behind a veil of anonymity.

#### **PART V – ORDER SOUGHT**

40. For the reasons stated above, it is respectfully submitted that this Honourable Court should order Teksavvy to, within 120 days of this Order, provide Voltage, in Microsoft Excel format, with the names, addresses, phone numbers, and email addresses of the Teksavvy customer accounts associated with the IP addresses attached as Exhibit “B” to the Affidavit of Barry Logan.

#### **PART VI – LIST OF AUTHORITIES**

*BMG Canada Inc. v. Doe*, 2005 FCA 193

*Voltage Pictures LLC v. Jane Doe*, 2011 FC 1024

*R. v. Brzezinski*, 2009 CarswellOnt 8689

*R. v. Ward*, 2012 ONCA 660

*R v. Trapp*, 2011 SKCA 143



Dated: December 11, 2012

**ALL OF WHICH IS RESPECTFULLY  
SUBMITTED**

  
\_\_\_\_\_  
**JAMES ZIBARRAS**

**BRAUTI THORNING ZIBARRAS LLP**  
151 Yonge Street, Suite 1800  
Toronto, ON M5C 2W7

**James Zibarras**  
**LSUC No. 48856F**

**John Philpott**  
**LSCU No. 60246U**

Tel: 416.362.4567  
Fax: 416.362.8410

Lawyers for the Plaintiff/Moving Party,  
**VOLTAGE PICTURES LLC**

## APPENDIX "A"

### Statutes and Regulations

---

#### FEDERAL COURT RULES

##### Examination of non-parties with leave

**238.** (1) A party to an action may bring a motion for leave to examine for discovery any person not a party to the action, other than an expert witness for a party, who might have information on an issue in the action.

##### Personal service on non-party

(2) On a motion under subsection (1), the notice of motion shall be served on the other parties and personally served on the person to be examined.

##### Where Court may grant leave

(3) The Court may, on a motion under subsection (1), grant leave to examine a person and determine the time and manner of conducting the examination, if it is satisfied that

(a) the person may have information on an issue in the action;

(b) the party has been unable to obtain the information informally from the person or from another source by any other reasonable means;

(c) it would be unfair not to allow the party an opportunity to question the person before trial; and

(d) the questioning will not cause undue delay, inconvenience or expense to the person or to the other parties.

#### REGLES DES COURS FEDERALES

##### Interrogatoire d'un tiers

**238.** (1) Une partie à une action peut, par voie de requête, demander l'autorisation de procéder à l'interrogatoire préalable d'une personne qui n'est pas une partie, autre qu'un témoin expert d'une partie, qui pourrait posséder des renseignements sur une question litigieuse soulevée dans l'action.

##### Signification de l'avis de requête

(2) L'avis de la requête visée au paragraphe (1) est signifié aux autres parties et, par voie de signification à personne, à la personne que la partie se propose d'interroger.

#### Autorisation de la Cour

(3) Par suite de la requête visée au paragraphe (1), la Cour peut autoriser la partie à interroger une personne et fixer la date et l'heure de l'interrogatoire et la façon de procéder, si elle est convaincue, à la fois :

- a)* que la personne peut posséder des renseignements sur une question litigieuse soulevée dans l'action;
- b)* que la partie n'a pu obtenir ces renseignements de la personne de façon informelle ou d'une autre source par des moyens raisonnables;
- c)* qu'il serait injuste de ne pas permettre à la partie d'interroger la personne avant l'instruction;
- d)* que l'interrogatoire n'occasionnera pas de retards, d'inconvénients ou de frais déraisonnables à la personne ou aux autres parties.

### **COPYRIGHT ACT**

#### Infringement generally

**27.** (1) It is an infringement of copyright for any person to do, without the consent of the owner of the copyright, anything that by this Act only the owner of the copyright has the right to do.

#### Secondary infringement

(2) It is an infringement of copyright for any person to

- (a)* sell or rent out,
- (b)* distribute to such an extent as to affect prejudicially the owner of the copyright,
- (c)* by way of trade distribute, expose or offer for sale or rental, or exhibit in public,
- (d)* possess for the purpose of doing anything referred to in paragraphs *(a)* to *(c)*, or
- (e)* import into Canada for the purpose of doing anything referred to in paragraphs *(a)* to *(c)*,

a copy of a work, sound recording or fixation of a performer's performance or of a communication signal that the person knows or should have known infringes copyright or would infringe copyright if it had been made in Canada by the person who made it.

### Liability for infringement

**35.** (1) Where a person infringes copyright, the person is liable to pay such damages to the owner of the copyright as the owner has suffered due to the infringement and, in addition to those damages, such part of the profits that the infringer has made from the infringement and that were not taken into account in calculating the damages as the court considers just.

### Proof of profits

(2) In proving profits,

(a) the plaintiff shall be required to prove only receipts or revenues derived from the infringement; and

(b) the defendant shall be required to prove every element of cost that the defendant claims.

### Statutory damages

**38.1** (1) Subject to this section, a copyright owner may elect, at any time before final judgment is rendered, to recover, instead of damages and profits referred to in subsection 35(1), an award of statutory damages for all infringements involved in the proceedings, with respect to any one work or other subject-matter, for which any one infringer is liable individually, or for which any two or more infringers are liable jointly and severally, in a sum of not less than \$500 or more than \$20,000 as the court considers just.

### Where defendant unaware of infringement

(2) Where a copyright owner has made an election under subsection (1) and the defendant satisfies the court that the defendant was not aware and had no reasonable grounds to believe that the defendant had infringed copyright, the court may reduce the amount of the award to less than \$500, but not less than \$200.

### Special case

(3) Where

(a) there is more than one work or other subject-matter in a single medium, and

(b) the awarding of even the minimum amount referred to in subsection (1) or (2) would result in a total award that, in the court's opinion, is grossly out of proportion to the infringement,

the court may award, with respect to each work or other subject-matter, such lower amount than \$500 or \$200, as the case may be, as the court considers just.

#### Collective societies

(4) Where the defendant has not paid applicable royalties, a collective society referred to in section 67 may only make an election under this section to recover, in lieu of any other remedy of a monetary nature provided by this Act, an award of statutory damages in a sum of not less than three and not more than ten times the amount of the applicable royalties, as the court considers just.

#### Factors to consider

(5) In exercising its discretion under subsections (1) to (4), the court shall consider all relevant factors, including

- (a) the good faith or bad faith of the defendant;
- (b) the conduct of the parties before and during the proceedings; and
- (c) the need to deter other infringements of the copyright in question.

#### No award

(6) No statutory damages may be awarded against

- (a) an educational institution or a person acting under its authority that has committed an act referred to in section 29.6 or 29.7 and has not paid any royalties or complied with any terms and conditions fixed under this Act in relation to the commission of the act;
- (b) an educational institution, library, archive or museum that is sued in the circumstances referred to in section 38.2; or
- (c) a person who infringes copyright under paragraph 27(2)(e) or section 27.1, where the copy in question was made with the consent of the copyright owner in the country where the copy was made.

#### Exemplary or punitive damages not affected

(7) An election under subsection (1) does not affect any right that the copyright owner may have to exemplary or punitive damages.

1997, c. 24, s. 20.

#### Offences and punishment

**42.** (1) Every person who knowingly

- (a) makes for sale or rental an infringing copy of a work or other subject-matter in which

copyright subsists,

(b) sells or rents out, or by way of trade exposes or offers for sale or rental, an infringing copy of a work or other subject-matter in which copyright subsists,

(c) distributes infringing copies of a work or other subject-matter in which copyright subsists, either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright,

(d) by way of trade exhibits in public an infringing copy of a work or other subject-matter in which copyright subsists, or

(e) imports for sale or rental into Canada any infringing copy of a work or other subject-matter in which copyright subsists

is guilty of an offence and liable

(f) on summary conviction, to a fine not exceeding twenty-five thousand dollars or to imprisonment for a term not exceeding six months or to both, or

(g) on conviction on indictment, to a fine not exceeding one million dollars or to imprisonment for a term not exceeding five years or to both.

## **LOI SUR LE DROIT D'AUTEUR**

### **Règle générale**

**27. (1)** Constitue une violation du droit d'auteur l'accomplissement, sans le consentement du titulaire de ce droit, d'un acte qu'en vertu de la présente loi seul ce titulaire a la faculté d'accomplir.

### **Violation à une étape ultérieure**

(2) Constitue une violation du droit d'auteur l'accomplissement de tout acte ci-après en ce qui a trait à l'exemplaire d'une oeuvre, d'une fixation d'une prestation, d'un enregistrement sonore ou d'une fixation d'un signal de communication alors que la personne qui accomplit l'acte sait ou devrait savoir que la production de l'exemplaire constitue une violation de ce droit, ou en constituerait une si l'exemplaire avait été produit au Canada par la personne qui l'a produit :

a) la vente ou la location;

b) la mise en circulation de façon à porter préjudice au titulaire du droit d'auteur;

c) la mise en circulation, la mise ou l'offre en vente ou en location, ou l'exposition en public, dans un but commercial;

d) la possession en vue de l'un ou l'autre des actes visés aux alinéas a) à c);

e) l'importation au Canada en vue de l'un ou l'autre des actes visés aux alinéas a) à c).

#### Violation du droit d'auteur : responsabilité

**35.** (1) Quiconque viole le droit d'auteur est passible de payer, au titulaire du droit qui a été violé, des dommages-intérêts et, en sus, la proportion, que le tribunal peut juger équitable, des profits qu'il a réalisés en commettant cette violation et qui n'ont pas été pris en compte pour la fixation des dommages-intérêts.

#### Détermination des profits

(2) Dans la détermination des profits, le demandeur n'est tenu d'établir que ceux provenant de la violation et le défendeur doit prouver chaque élément du coût qu'il allègue.

#### Dommages-intérêts préétablis

**38.1** (1) Sous réserve du présent article, le titulaire du droit d'auteur, en sa qualité de demandeur, peut, avant le jugement ou l'ordonnance qui met fin au litige, choisir de recouvrer, au lieu des dommages-intérêts et des profits visés au paragraphe 35(1), des dommages-intérêts préétablis dont le montant, d'au moins 500 \$ et d'au plus 20 000 \$, est déterminé selon ce que le tribunal estime équitable en l'occurrence, pour toutes les violations — relatives à une oeuvre donnée ou à un autre objet donné du droit d'auteur — reprochées en l'instance à un même défendeur ou à plusieurs défendeurs solidairement responsables.

#### Cas particuliers

(2) Dans les cas où le défendeur convainc le tribunal qu'il ne savait pas et n'avait aucun motif raisonnable de croire qu'il avait violé le droit d'auteur, le tribunal peut réduire le montant des dommages-intérêts préétablis jusqu'à 200 \$.

#### Cas particuliers

(3) Dans les cas où plus d'une oeuvre ou d'un autre objet du droit d'auteur sont incorporés dans un même support matériel, le tribunal peut, selon ce qu'il estime équitable en l'occurrence, réduire, à l'égard de chaque oeuvre ou autre objet du droit d'auteur, le montant minimal visé au paragraphe (1) ou (2), selon le cas, s'il est d'avis que même s'il accordait le montant minimal de dommages-intérêts préétablis le montant total de ces dommages-intérêts serait extrêmement disproportionné à la violation.

#### Société de gestion

(4) Si le défendeur n'a pas payé les redevances applicables en l'espèce, la société de gestion visée à l'article 67 — au lieu de se prévaloir de tout autre recours en vue d'obtenir un redressement pécuniaire prévu par la présente loi — ne peut, aux termes du présent article, que choisir de recouvrer des dommages-intérêts préétablis dont le montant, de trois à dix fois le montant de ces redevances, est déterminé selon ce que le tribunal estime équitable en l'occurrence.

#### Facteurs

(5) Lorsqu'il rend une décision relativement aux paragraphes (1) à (4), le tribunal tient compte notamment des facteurs suivants :

- a) la bonne ou mauvaise foi du défendeur;
- b) le comportement des parties avant l'instance et au cours de celle-ci;
- c) la nécessité de créer un effet dissuasif à l'égard de violations éventuelles du droit d'auteur en question.

Cas où les dommages-intérêts préétablis ne peuvent être accordés

(6) Ne peuvent être condamnés aux dommages-intérêts préétablis :

- a) l'établissement d'enseignement ou la personne agissant sous l'autorité de celui-ci qui a fait les actes visés aux articles 29.6 ou 29.7 sans acquitter les redevances ou sans observer les modalités afférentes fixées sous le régime de la présente loi;
- b) l'établissement d'enseignement, la bibliothèque, le musée ou le service d'archives, selon le cas, qui est poursuivi dans les circonstances prévues à l'article 38.2;
- c) la personne qui commet la violation visée à l'alinéa 27(2)e) ou à l'article 27.1 dans les cas où la reproduction en cause a été faite avec le consentement du titulaire du droit d'auteur dans le pays de production.

#### Dommages-intérêts exemplaires

(7) Le choix fait par le demandeur en vertu du paragraphe (1) n'a pas pour effet de supprimer le droit de celui-ci, le cas échéant, à des dommages-intérêts exemplaires ou punitifs.

#### Infractions et peines

**42.** (1) Commet une infraction quiconque, sciemment :

- a) se livre, en vue de la vente ou de la location, à la contrefaçon d'une oeuvre ou d'un autre objet du droit d'auteur protégés;



*b)* en vend ou en loue, ou commercialement en met ou en offre en vente ou en location un exemplaire contrefait;

*c)* en met en circulation des exemplaires contrefaits, soit dans un but commercial, soit de façon à porter préjudice au titulaire du droit d'auteur;

*d)* en expose commercialement en public un exemplaire contrefait;

*e)* en importe pour la vente ou la location, au Canada, un exemplaire contrefait.

Le contrevenant encourt, sur déclaration de culpabilité par procédure sommaire, une amende maximale de vingt-cinq mille dollars et un emprisonnement maximal de six mois, ou l'une de ces peines, ou, sur déclaration de culpabilité par voie de mise en accusation, une amende maximale d'un million de dollars et un emprisonnement maximal de cinq ans, ou l'une de ces peines.

**VOLTAGE PICTURES LLC**  
Plaintiff/Moving Party

and

**JOHN DOE AND JANE DOE**  
Defendants

**FEDERAL COURT**

Proceeding commenced at Toronto

**MEMORANDUM OF FACT AND LAW**

**BRAUTI THORNING ZIBARRAS LLP**  
151 Yonge Street, Suite 1800  
Toronto, ON M5C 2W7

**James Zibarras**  
**LSUC No. 48856F**

**John Philpott**  
**LSUC No. 60246U**

Tel.: 416.362.4567  
Fax: 416.362.8410

Lawyers for the Plaintiff/Moving Party,  
**VOLTAGE PICTURES LLC**

2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [ 2005] 4 F.C.R. 81

BMG Canada Inc. v. John Doe

BMG Canada Inc., EMI Music Canada, A Division of EMI Group Canada Inc., Sony Music Entertainment (Canada) Inc., Universal Music Canada Inc., Warner Music Canada Ltd., BMG Music, Arista Records Inc., Zomba Recording Corporation, EMI Music Sweden AB, Capitol Records, Inc., Chrysalis Records Limited, Virgin Records Limited, Sony Music Entertainment Inc., Sony Music Entertainment (UK) Inc., UMG Recordings, Inc., Mercury Records Limited and WEA International Inc., Appellants - Plaintiffs and John Doe, Jane Doe and All those Persons who are Infringing Copyright in the Plaintiffs' Sound Recordings, Defendants and Shaw Communications Inc., Roger Cable Communications Inc., Bell Canada, Telus Inc. and Videotron Ltee., Respondents / Third Party Respondents and The Canadian Internet Policy and Public Interest Clinic, Intervener

Federal Court of Appeal

Noël J.A., Richard C.J., Sexton J.A.

Heard: April 20-21, 2005

Judgment: May 19, 2005

Docket: A-203-04

© Thomson Reuters Canada Limited or its Licensors (excluding individual court documents). All rights reserved.

Proceedings: affirming *BMG Canada Inc. v. John Doe* (2004), [2004] 3 F.C.R. 241, 239 D.L.R. (4th) 726, 2004 CF 488, 32 C.P.R. (4th) 64, 2004 CarswellNat 2774, 250 F.T.R. 267, 2004 CarswellNat 835, 2004 FC 488 (F.C.)

Counsel: Mr. Harry Radomski, Mr. Richard Naiberg, Mr. Peter Ruby, for Appellants

Mr. James Hodgson, Mr. Jeffrey Percival, for Respondent, Bell Canada

Ms Wendy Matheson, Ms Amanda Kemshaw, for Respondent, Rogers Cable

Mr. Charles Scott, Mr. Rocco Di Pucchio, for Respondent, Shaw Communications

Mr. Joel Watson, for Respondent, Telus Communications

Mr. J. Serge Sasseville, for Respondent, Videotron

Mr. Howard Knopf, Mr. Alex Cameron, for Intervener, The Canadian Internet Policy and Public Interest Clinic, CIPPIC

Subject: Civil Practice and Procedure; Intellectual Property; Corporate and Commercial

Civil practice and procedure --- Discovery — Discovery of documents — Scope of documentary discovery — Documents in possession of non-party — General principles

2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

Plaintiffs were largest music producers in Canada — Plaintiffs brought action against 29 internet users who allegedly downloaded more than 1,000 songs over which producers had rights under Copyright Act onto their home computers — Plaintiffs were unable to determine name, address or telephone number of defendants as they operated under pseudonyms — Defendants used internet protocol ("IP") addresses registered with internet service providers ("ISPs") — Plaintiffs' motion, seeking disclosure from five Canadian ISPs, who were not parties to action, of identity of certain customers who allegedly infringed copyright laws by trading in music downloaded from internet, was dismissed — Motions judge found that motion was in essence equitable bill of discovery — Motions judge stated that to meet test for granting bill of discovery, applicant must establish prima facie case, person from whom information was sought must be involved in disputed matter, person must be only practical source of information, person must be reasonably compensated for compliance expenses, and public interest in favour of disclosure must outweigh legitimate expectation of privacy — Motions judge determined that plaintiffs failed to establish prima facie case — Motions judge found no evidence of connection between pseudonyms and IP addresses — Motions judge found no evidence that ISPs were only practical source of information available — Motions judge held that process that was sought to be imposed on ISPs would be costly and would divert their resources from other tasks — Motions judge determined that given age of data sought, its unreliability and serious possibility of innocent account holder being identified, privacy concerns outweighed public interest concerns favouring disclosure — Plaintiffs appealed — Appeal dismissed without prejudice to plaintiffs' right to commence further application — Motions judge erred in finding that plaintiffs were required to establish prima facie case — At such preliminary stage of proceedings, plaintiffs did not know identity of persons they wished to sue, let alone details of precisely what was done by each of them such as to actually prove infringement — Plaintiffs were only required to show bona fide claim such that they really did intend to bring action for infringement of copyright based upon information they obtain, and that there was no other improper purpose for seeking identity of users — Motions judge did not err in his findings with respect to remaining criteria for granting equitable bill of discovery.

Intellectual property --- Copyright --- Infringement of owner's rights — Direct infringement — Reproduction and copying — General principles

Plaintiffs were largest music producers in Canada — Plaintiffs brought action against 29 internet users who allegedly downloaded more than 1,000 songs over which producers had rights under Copyright Act onto their home computers — Plaintiffs were unable to determine name, address or telephone number of defendants as they operated under pseudonyms — Defendants used internet protocol ("IP") addresses registered with internet service providers ("ISPs") — Plaintiffs' motion, seeking disclosure from five Canadian ISPs, who were not parties to action, of identity of certain customers who allegedly infringed copyright laws by trading in music downloaded from internet, was dismissed — Motions judge found no evidence of infringement of copyright — Motions judge determined that downloading song for personal use did not amount to infringement as s. 80(1) of Copyright Act provides that act of reproducing musical work onto audio recording for private use of person who makes copy does not constitute infringement of copyright — Motions judge found no evidence that alleged infringers either distributed or authorized reproduction of sound recordings — Motions judge held that mere fact of placing copy on shared directory in computer where that copy can be accessed did not amount to distribution — Plaintiffs appealed — Appeal dismissed without prejudice to plaintiffs' right to commence further application — Motions judge's conclusions with respect to copyright infringement should not have been made at that stage of proceedings since not all evidence was available, nor were all applicable legal principles considered — If case were to proceed further, it should be done so on basis that no findings on issue of infringement were made.

**Cases considered by *Sexton J.A.*:**

*British Steel Corp. v. Granada Television Ltd.* (1981), [1981] 1 All E.R. 417, [1981] A.C. 1096 (Eng. Ch. Div.) — considered

*Canadian Private Copying Collective v. Canadian Storage Media Alliance* (2004), 2004 CAF 424, 2004 CarswellNat 5345, 36 C.P.R. (4th) 289, 247 D.L.R. (4th) 193, 329 N.R. 101, 2004 FCA 424, 2004 CarswellNat 4681 (F.C.A.) — referred to

*CCH Canadian Ltd. v. Law Society of Upper Canada* (2004), 247 F.T.R. 318 (note), 236 D.L.R. (4th) 395, 317 N.R. 107,

2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

30 C.P.R. (4th) 1, [2004] 1 S.C.R. 339, 2004 SCC 13, 2004 CarswellNat 446, 2004 CarswellNat 447 (S.C.C.) — referred to

*Glaxo Wellcome plc v. Minister of National Revenue* (1998), 162 D.L.R. (4th) 433, 1998 CarswellNat 1388, 228 N.R. 164, 20 C.P.C. (4th) 243, 81 C.P.R. (3d) 372, 147 F.T.R. 309 (note), [1998] 4 F.C. 439, 7 Admin. L.R. (3d) 147, 1998 CarswellNat 2801 (Fed. C.A.) — followed

*Housen v. Nikolaisen* (2002), 2002 SCC 33, 2002 CarswellSask 178, 2002 CarswellSask 179, 286 N.R. 1, 10 C.C.L.T. (3d) 157, 211 D.L.R. (4th) 577, [2002] 7 W.W.R. 1, 219 Sask. R. 1, 272 W.A.C. 1, 30 M.P.L.R. (3d) 1, [2002] 2 S.C.R. 235 (S.C.C.) — referred to

*Indian Manufacturing Ltd. v. Lo* (1996), 199 N.R. 114, 68 C.P.R. (3d) 174, 1996 CarswellNat 712 (Fed. C.A.) — referred to

*Irwin Toy Ltd. v. Joe Doe* (2000), 2000 CarswellOnt 3164, 12 C.P.C. (5th) 103 (Ont. S.C.J.) — considered

*Johnston v. Frank Johnston's Restaurants Ltd.* (1980), 33 Nfld. & P.E.I.R. 341, 93 A.P.R. 341, 1980 CarswellPEI 82, 109 D.L.R. (3d) 227 (P.E.I. C.A.) — considered

*Loblaws Cos. v. Aliant Telecom Inc.* (2003), 2003 NBQB 215, 2003 CarswellNB 234 (N.B. Q.B.) — considered

*Norwich Pharmacal Co. v. Customs & Excise Commissioners* (1973), [1974] A.C. 133, [1973] 2 All E.R. 943, [1973] 3 W.L.R. 164, [1974] R.P.C. 101 (U.K. H.L.) — considered

*Straka v. Humber River Regional Hospital* (2000), 2000 CarswellOnt 4114, 51 O.R. (3d) 1, 193 D.L.R. (4th) 680, 137 O.A.C. 316, 1 C.P.C. (5th) 195 (Ont. C.A.) — considered

#### Statutes considered:

*Copyright Act*, R.S.C. 1985, c. C-42

Generally — referred to

s. 27(2) — referred to

s. 27(2)(b) — referred to

s. 27(2)(d) — referred to

s. 80(1) — considered

s. 80(2) — considered

*Customs Act*, R.S.C. 1985, c. 1 (2nd Supp.)

Generally — referred to

*Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5

2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

Generally — referred to

s. 3 — referred to

s. 7(3) — referred to

s. 7(3)(c) — referred to

s. 8(8) — referred to

s. 28 — referred to

**Rules considered:**

*Federal Court Rules, 1998, SOR/98-106*

R. 81 — considered

R. 136 — considered

R. 233 — considered

R. 233(1) — referred to

R. 238 — considered

R. 238(1) — considered

R. 238(2) — considered

R. 238(3) — considered

*Rules of Civil Procedure, R.R.O. 1990, Reg. 194*

R. 30.10 — referred to

R. 31.10 — referred to

R. 32.12 — referred to

APPEAL by recording industry producers from judgment reported at *BMG Canada Inc. v. John Doe* (2004), [2004] 3 F.C.R. 241, 239 D.L.R. (4th) 726, 2004 CF 488, 32 C.P.R. (4th) 64, 2004 CarswellNat 2774, 250 F.T.R. 267, 2004 CarswellNat 835, 2004 FC 488 (F.C.), dismissing motion against internet service providers for identity of certain customers who allegedly have infringed copyright laws.

**Sexton J.A.:**

2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

## Introduction

1 This case illustrates the tension existing between the privacy rights of those who use the Internet and those whose rights may be infringed or abused by anonymous Internet users.

2 Canada's music producers and recording industry are very concerned about infringement of copyright in their musical works through the use of Internet file sharing. They maintain that the industry, including the creators of the musical works, lose millions of dollars every year in sales due to the unauthorized downloading of files. They wish to bring action against the infringers but do not have their identity. They allege that the only means of ascertaining the identity is through the Internet Service Providers (ISPs), who provide the internet service to the infringers.

3 The ISPs, citing privacy concerns, have refused to provide the names of the Internet users, who are downloading files of the recording industry, without a court order.

4 Citizens legitimately worry about encroachment upon their privacy rights. The potential for unwarranted intrusion into individual personal lives is now unparalleled. In an era where people perform many tasks over the Internet, it is possible to learn where one works, resides or shops, his or her financial information, the publications one reads and subscribes to and even specific newspaper articles he or she has browsed. This intrusion not only puts individuals at great personal risk but also subjects their views and beliefs to untenable scrutiny. Privacy advocates maintain that if privacy is to be sacrificed, there must be a strong *prima facie* case against the individuals whose names are going to be released. Whether this is the correct test will be addressed in this decision.

5 Ultimately the issue is whether the identity of persons who are alleged to infringe musical copyright can be revealed despite the fact that their right to privacy may be violated. Each side presents compelling arguments and the difficulty lies in reaching a balance between the competing interests.

## Facts

6 The plaintiffs consist of the largest musical providers in Canada and claim to collectively own the Canadian copyrights in more than 80% of the sound recordings sold to the public in Canada.

7 The plaintiffs claim that 29 internet users have each downloaded more than 1000 songs (the Songs) over which the plaintiffs have copyright onto their home computers and, by means of what is called a "peer-to-peer" (P2P) file sharing program, are infringing the plaintiffs' copyright by providing access to their files, thus reproducing or distributing the plaintiffs' Songs to countless other Internet users. The persons are alleged to be using 29 distinct Internet locations (IP addresses) to carry out their infringing activities.

8 The respondents are ISPs who administer the 29 IP addresses and are said to be the only entities who have information regarding the identity of the 29 persons.

9 The plaintiffs are unable to determine the name, address or telephone number of any of the 29 internet users in question as they operate under pseudonyms associated with software which they use; e.g., Geekboy@KaZaA. However, they have conducted an investigation, through which, they submit, it was discovered that these individuals used IP addresses registered with the ISPs. The plaintiffs sought an order, pursuant to Rules 233 and 238 of the *Federal Court Rules, 1998*, SOR/98-106 (Rules), to compel the ISPs to disclose the names of the customers who used the 29 IP addresses at times material to these proceedings. The respondents had previously refused to provide the information voluntarily.

10 The plaintiffs wish to pursue litigation against these 29 individuals but being unaware of their identities, they commenced this action against "John Doe, Jane Doe and all those persons who are infringing copyright in the plaintiffs' sound recordings" and then brought this motion before the Federal Court to identify these 29 individuals.



2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

11 On the motion, the plaintiffs filed affidavits of Gary Millin, President of MediaSentry Inc. (MediaSentry), a company that provides online anti-piracy protection by specializing in automated detection of the unauthorized distribution of copyrighted materials on the Internet. The plaintiffs had retained MediaSentry to investigate file-sharing of the Songs.

12 The affidavits explained that the plaintiffs provided a list of the Songs to MediaSentry. MediaSentry through its computer program then searched the Internet and identified 29 IP addresses as addresses from which large numbers of sound recordings, including the Songs, were being offered for copying. Screenshots were saved showing the numerous files being offered at these IP addresses. Copies of the files were then requested and received from these IP addresses. MediaSentry's program also matched each of the 29 IP addresses to the specific ISP who administered each IP address at the relevant time. MediaSentry provided the files it received to a representative of the plaintiffs who confirmed that the contents of these files corresponded with the Songs.

13 The ISPs responded in different ways. Shaw, Bell and Telus argued that cross-examination showed that the affidavits were hearsay and not in compliance with Rule 81 of the Rules, maintaining *inter alia* that Mr. Millin had not done the investigation personally and had not revealed his sources of information and hence his evidence could not be accepted. Most importantly, they argued that because the evidence was hearsay, the plaintiffs had failed to establish any connection between the pseudonyms from which MediaSentry extracted the sound recordings on the Internet (i.e. Geekboy@KaZaA) and the IP addresses connected to the various respondent. Further, Shaw and Telus argued that under Rule 238 and the principles relating to equitable bills of discovery, that the plaintiffs had failed to establish a *prima facie* case of infringement and therefore no discovery could be ordered. They also argued that it would be burdensome and expensive to extract the information from their records. They along with the respondent, Rogers, maintained that the information would be stale dated and hence unreliable due to the delay between the time they were being asked to provide the information and the time when MediaSentry did their investigation. This fed their concerns about protecting the privacy of their customers whom they were obliged to protect by virtue of the *Personal Information Protection and Electronic Documents Act*, 2000, c. 5 (PIPEDA). Videotron agreed with the plaintiffs' submissions on copyright infringement and adopted them as its own. Finally, while Bell and Videotron had privacy concerns, they indicated they were able to produce the information requested without difficulty but would not do so without a court order in view of PIPEDA.

14 The motion was dismissed by the Federal Court.

15 The Motions Judge held that:

a) Rule 233 was not applicable because it presupposes the existence of specified documents. Here, the documents that would reveal the identity of the 29 persons did not pre-exist. Rather, documents containing the information would have to be created by the respondents through the use of existing logs and tapes.

b) The affidavits filed in support of the motion were deficient in that the evidence failed to satisfy the requirements of Rule 81 because "major portions of these affidavits are based upon information which Mr. Millin gained from his employees. Accordingly they consist largely of hearsay.... Mr. Millin gives no reason for his beliefs."

c) Because of the conclusions in (a) and (b), there was no clear evidence that the requisite relationship between the IP addresses and the pseudonyms had been established.

d) Although the plaintiffs brought the motion pursuant to Rule 238, the legal principles applicable to equitable bills of discovery should apply to applications under Rule 238.

e) The test articulated by the Motions Judge for granting an equitable bill of discovery was as follows:

#### **Equitable Bill of Discovery Requirements**



2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

- (a) the applicant must establish a *prima facie* case against the unknown alleged wrongdoer;
- (b) the person from whom discovery is sought must be in some way involved in the matter under dispute, he must be more than an innocent bystander;
- (c) the person from whom discovery is sought must be the only practical source of information available to the applicants;
- (d) the person from whom discovery is sought must be reasonably compensated for his expenses arising out of compliance with the discovery order in addition to his legal costs;
- (e) the public interests in favour of disclosure must outweigh the legitimate privacy concerns.

f) With respect to Criterion (a) of the equitable bill of discovery requirements, the Motions Judge found that the affidavits were also deficient in that they did not establish a *prima facie* case of infringement of copyright. In this connection the Motions Judge embarked upon a consideration of whether there had been an infringement of copyright. He said inter alia, at paragraphs 25 to 29:

Thus, downloading a song for personal use does not amount to infringement. See *Copyright Board of Canada, Private Copying 2003-2004 decision*, 12 December 2003 at page 20.

No evidence was presented that the alleged infringers either distributed or authorized the reproduction of sound recordings. They merely placed personal copies into their shared directories which were accessible by other computer users via a P2P service.

As far as authorization is concerned, the case of *CCH Canada Ltd. v. Law Society of Canada*, 2004 SCC 13, established that setting up the facilities that allow copying does not amount to authorizing infringement. I cannot see a real difference between a library that places a photocopy machine in a room full of copyrighted material and a computer user that places a personal copy on a shared directory linked to a P2P service. In either case the preconditions to copying and infringement are set up but the element of authorization is missing....

The mere fact of placing a copy on a shared directory in a computer where that copy can be accessed via a P2P service does not amount to distribution. Before it constitutes distribution, there must be a positive act by the owner of the shared directory, such as sending or the copies or advertising that they are available for copying. No such evidence was presented by the plaintiffs in this case. They merely presented evidence that the alleged infringers made copies available on their shared drives. The exclusive right to make available is included in the *World Intellectual Property Organization Performances and Phonograms Treaty*, (WPPT), 20/12/1996 (CRNR/DC/95, December 23, 1996), however that treaty has not yet been implemented in Canada and therefore does not form part of Canadian copyright law.

Lastly, while the plaintiffs allege that there was secondary infringement contrary to s. 27(2) of the *Copyright Act*, they presented no evidence of knowledge on the part of the infringer. Such evidence of knowledge is a necessary condition for establishing infringement under that section.

g) The Motions Judge found that the plaintiffs met the requirements of Criterion (b) of the equitable bill of discovery principles relating to the involvement of the ISPs.

h) With respect to Criterion (c), the Motions Judge found that he was not satisfied that the information could not have been

2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

obtained from the operators of the web sites named (i.e. KaZaA, *et al*).

i) With respect to Criterion (d), the respondents would have to be compensated for their expenses if an order were granted.

j) Finally, with respect to Criterion (e), because of the age of the data and its consequent unreliability, the privacy interests of the 29 persons outweighed the public interest concern in favour of disclosure.

## Analysis

### Standard of Review

16 The standard of review on questions of law, such as the correct tests to be applied with respect to the granting of equitable bills of discovery or the interpretation of the *Federal Court Rules*, is correctness. The standard of review with respect to findings of fact involves a consideration of whether the judge made a palpable and overriding error. See *Housen v. Nikolaisen*, [2002] 2 S.C.R. 235 (S.C.C.), at 248, 252, and 256.

### Rule 233

17 I can find no palpable and overriding error in the conclusions of the Motions Judge with respect to Rule 233.

18 Rule 233(1) states,

233. (1) On motion, the Court may order the production of any document that is in the possession of a person who is not a party to the action, if the document is relevant and its production could be compelled at trial.

233. (1) La Cour peut, sur requête, ordonner qu'un document en la possession d'une personne qui n'est pas une partie à l'action soit produit s'il est pertinent et si sa production pourrait être exigée lors de l'instruction.

19 The information sought by the plaintiffs may be buried in logs and tapes but is not presently in a readable format. Since the documents in a readable format do not currently exist and would have to be created, Rule 233 has no application. The Rule contemplates the production of documents which are "in the possession of a person". It cannot be said that documents which do not exist are in the possession of a person.

### Rule 81

20 I am of the view that the Motions Judge made no palpable and overriding error in concluding that the plaintiffs' material was deficient in that it failed to comply with Rule 81.

81. (1) Affidavits shall be confined to facts within the personal knowledge of the deponent, except on motions in which statements as to the deponent's belief, with the grounds therefor, may be included.

(2) Where an affidavit is made on belief, an adverse inference may be drawn from the failure of a party to provide evidence of persons having personal knowledge of material facts.

81. (1) Les affidavits se limitent aux faits dont le déclarant a une connaissance personnelle, sauf s'ils sont présentés à l'appui d'une requête, auquel cas ils peuvent contenir des déclarations fondées sur ce que le déclarant croit être les faits, avec motifs à l'appui.

(2) Lorsqu'un affidavit contient des déclarations fondées sur ce que croit le déclarant, le fait de ne pas offrir le témoignage de personnes ayant une connaissance personnelle des faits substantiels peut donner lieu à des conclusions défavorables.

2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

21 Much of the crucial evidence submitted by the plaintiffs was hearsay and no grounds are provided for accepting that hearsay evidence. In particular, the evidence purporting to connect the pseudonyms with the IP addresses was hearsay thus creating the risk that innocent persons might have their privacy invaded and also be named as defendants where it is not warranted. Without this evidence there is no basis upon which the motion can be granted and for this reason alone the appeal should be dismissed.

22 However the reasons of the Motions Judge extend beyond merely dealing with the hearsay evidence issue. Rather the reasons address such matters as the appropriate procedure necessary to obtain the identities of the users, the proper test to be applied by the Court in granting orders compelling disclosure of the identities, and vital copyright infringement issues. It is therefore necessary to address these issues.

### Rule 238

23 In spite of the arguments of the respondents, I believe this proceeding could be brought pursuant to Rule 238 of the Rules.

238. (1) A party to an action may bring a motion for leave to examine for discovery any person not a party to the action, other than an expert witness for a party, who might have information on an issue in the action.

(2) On a motion under subsection (1), the notice of motion shall be served on the other parties and personally served on the person to be examined.

(3) The Court may, on a motion under subsection (1), grant leave to examine a person and determine the time and manner of conducting the examination, if it is satisfied that

- (a) the person may have information on an issue in the action;
- (b) the party has been unable to obtain the information informally from the person or from another source by any other reasonable means;
- (c) it would be unfair not to allow the party an opportunity to question the person before trial; and
- (d) the questioning will not cause undue delay, inconvenience or expense to the person or to the other parties.

238. (1) Une partie à une action peut, par voie de requête, demander l'autorisation de procéder à l'interrogatoire préalable d'une personne qui n'est pas une partie, autre qu'un témoin expert d'une partie, qui pourrait posséder des renseignements sur une question litigieuse soulevée dans l'action.

(2) L'avis de la requête visée au paragraphe (1) est signifié aux autres parties et, par voie de signification à personne, à la personne que la partie se propose d'interroger.

(3) Par suite de la requête visée au paragraphe (1), la Cour peut autoriser la partie à interroger une personne et fixer la date et l'heure de l'interrogatoire et la façon de procéder, si elle est convaincue, à la fois :

- a) que la personne peut posséder des renseignements sur une question litigieuse soulevée dans l'action;
- b) que la partie n'a pu obtenir ces renseignements de la personne de façon informelle ou d'une autre source par des moyens raisonnables;
- c) qu'il serait injuste de ne pas permettre à la partie d'interroger la personne avant l'instruction;
- d) que l'interrogatoire n'occasionnera pas de retards, d'inconvénients ou de frais déraisonnables à la personne ou aux autres parties.

24 Rule 238(2) provides that notice of the motion must be served "on the other parties". Since the identities of the other parties are presently unknown to the plaintiffs, service is not possible and the respondents argued, therefore, that Rule 238 does not provide a procedure to discover the identities. Furthermore, they argued that Rule 238 is contained in a section under the general heading "Examination for Discovery" and that one would not normally expect the identity of each defendant to be revealed for the first time on an examination for discovery.

25 However, the plaintiffs argued that the main issue on the motion was the identity of each person who is committing infringement of the plaintiffs' copyrights. I agree and find that because this issue inevitably falls within the words in Rule

2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

238(1) as being "an issue in the action", Rule 238 is broad enough to permit discovery in cases such as this.

26 As to the respondent's arguments, there is provision in the Rules to deal with the matter of service. Rule 136 allows the court to order substituted service or to dispense with service altogether. This Court has used the previously equivalent Rule to order substituted service where the persons whom the appellants sought to serve, had no address. The substituted service there consisted of providing notice of the appeal through newspaper publication (*Indian Manufacturing Ltd. v. Lo* (1996), 68 C.P.R. (3d) 174 (Fed. C.A.)). Also, although it is true that examinations for discovery of a third party are not routinely ordered, and should not become common place, they nevertheless are clearly applicable and necessary in cases where the plaintiffs will be frustrated from pursuing their actions because they are unaware of the identity of the people they wish to sue. Furthermore, under Rule 238(3), the court may determine "the manner of conducting the examination". Thus a court could, in cases such as the present, limit the discovery to the submission of written questions which could be followed by written answers, limited to revealing only the identity of the users complained of, or such other limitations as the court might consider necessary.

27 It is worth noting that in *Irwin Toy Ltd. v. Joe Doe*, [2000] O.J. No. 3318 (Ont. S.C.J.), the Ontario Superior Court of Justice indicated that rules 30.10 and 31.10 of the *Rules of Civil Procedure*, R.R.O. 1990, Reg. 194, which are comparable to Rule 238, could be used to compel production of the identity of senders of e-mail from ISPs. There, the moving party successfully brought a motion to compel production of the identity of an individual who had sent an e-mail publication containing defamatory statements about the individual plaintiff. Similarly, in *Loblaw Cos. v. Aliant Telecom Inc.*, [2003] N.B.J. No. 208 (N.B. Q.B.), the New Brunswick Court of Queen's Bench used Rule 32.12 of the *New Brunswick Rules of Court*, N.B. Reg. 82-73, also comparable to Rule 238, to compel production of the identity of an individual who had sent an e-mail containing confidential payroll information about a number of senior Loblaw employees to thirty-four other employees of Loblaw. Loblaw sought the identity of the person because spreading confidential information could have given rise to an action for damages or for an injunction against the individual who circulated the information.

### Equitable Bills of Discovery

28 An equitable bill of discovery is an equitable remedy that is discretionary in nature. In Lord Denning's words in *British Steel Corp. v. Granada Television Ltd.*, [1981] 1 All E.R. 417 (Eng. Ch. Div.) at p. 439, the bill of discovery "enables a person, who has been injured by wrongdoing, to bring an action to discover the name of the wrongdoer".

29 The concept has been accepted by this Court in *Glaxo Wellcome plc v. Minister of National Revenue* (1998), 81 C.P.R. (3d) 372 (Fed. C.A.) and was explained by Stone J.A. at paragraph 20:

The equitable bill of discovery is in essence a form of pre-action discovery... It is of ancient origin. It developed alongside the procedures for discovery which are ordinarily available in the course of litigation and which, it is worth noting, also originated in the courts of equity.... This remedy permits a court, acting through its equitable jurisdiction, to order discovery of a person against whom the applicant for the bill of discovery has no cause of action and who is not a party to contemplated litigation. While it appears that an independent action for discovery cannot be brought against a person who is in the position of a "mere witness" or bystander to the cause of action, the case law suggests that a bill of discovery may be issued against an individual who is in some way connected to or involved in the misconduct.

30 The Motions Judge, while finding that the motion was brought pursuant to Rule 238, went on to hold that the criteria for determining whether an equitable bill of discovery should be issued, would be equally applicable to a proceeding brought under Rule 238. I agree. In my view, the plaintiffs could invoke either Rule 238 or equitable bills of discovery and in either case, the legal principles relating to equitable bills of discovery would be applicable. The same issues are at stake in both procedures and there would seem to be no reason for not applying the same legal principles.

31 While I agree that the criteria relating to granting an equitable bill of discovery can be applied to a Rule 238 motion in cases such as this, I disagree with the description of the first aspect of the test made by the Motions Judge. He said that the plaintiff has to provide evidence of a *prima facie* case. The plaintiffs argued that this was the wrong test and that the proper test



2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

should be whether the plaintiff has a *bona fide* claim against the proposed defendant. The respondents said that the plaintiffs had argued before the Motions Judge that the *prima facie* test was the correct one and that they should not be allowed to take a different position on appeal. If the respondents are correct as to what was argued before the Motions Judge, this might explain why he adopted the *prima facie* test. In any event, it is the duty of this Court to get the test right regardless of what was or is argued by counsel.

32 I am of the view that the proper test is whether the plaintiff has a *bona fide* claim against the proposed defendant. This is the test enunciated by this Court in *Glaxo, supra*, on very similar facts, after it considered *Norwich Pharmacal Co. v. Customs & Excise Commissioners* (1973), [1974] A.C. 133 (U.K. H.L.), where the test was reviewed by the House of Lords. In *Glaxo, supra*, the appellant sought disclosure of the names of individuals whose identity was unknown to Glaxo and who it was alleged had imported certain drugs into Canada, having the effect of infringing Glaxo's patent. Glaxo sought the names of the importers from Revenue Canada who were said to have the required information for the purposes of the *Customs Act*, R.S. 1985, c. 1 (2<sup>nd</sup> Supp.). An order was granted for disclosure. In his decision, Stone J.A. said at paragraphs 30 and 44:

It is of interest to note that several Canadian courts have adopted the Norwich Pharmacal approach to interpreting their own rules of civil procedure authorizing pre-action discovery.<sup>14</sup> See for example Rule 18.02(c) of Nova Scotia's Civil Procedure Rules and Rule 18.02(1)(c) of Prince Edward Island's Rules of Civil Procedure.<sup>14</sup> For instance, the Prince Edward Island Court of Appeal in *Re Johnston and Frank Johnston's Restaurants Limited* (1980), 33 Nfld. & P.E.I.R. 341 at pages 348, 351 and 353, specified three main criteria which an applicant must satisfy in order to be entitled to discover a third party before launching legal proceedings. The applicant must demonstrate that he or she has a bona fide claim. The Court added that the applicant's claim must be likely to succeed at trial, which according to my reading of the decision in *Norwich Pharmacal* was not an invariable requirement enunciated by the House of Lords. In an action for the infringement of patent rights, quite apart from a general denial, a defence of invalidity is often raised on the ground of lack of novelty, obviousness, insufficiency of specification or claims or some other recognized basis.<sup>15</sup> See R.T. Hughes and J.H. Woodley, *Hughes and Woodley on Patents* (Toronto: Butterworths, 1984) at paragraph 36.15 It seems to me to go too far to insist that with respect to this kind of anticipated litigation, an applicant for a bill of discovery must show that he or she is likely to succeed at trial. As we have already seen, Lord Cross of Chelsea required that "the strength of the applicant's case" be considered as a factor, while Lord Kilbrandon spoke only of disclosing the names of persons "whom the appellants bona fide believe to be infringing" their patent rights. Finally, the applicant must also establish that he or she shares some sort of relationship with the third party against whom discovery is sought (i.e. that the person is in some way involved in the wrongdoing), and that the third party is the only practicable source of information available. These three requirements were likewise endorsed by the Nova Scotia Supreme Court in *Comeau, Re* (1986), 77 N.S.R. (2d) 57 at pages 59-60, and in *Leahy v. Dr. A.B.* (1992), 113 N.S.R. (2d) 417 at page 419. (emphasis added)

The next task is to determine whether the appellant has satisfied the criteria for issuing a bill of discovery. To my mind, the principles articulated in *Norwich Pharmacal, supra*, have direct application to the circumstances of the present case. Turning now to those principles, in my view the appellant has satisfied the threshold requirement for a bill of discovery in that it has a bona fide or legitimate claim against those who are importing RHCL into the country. (emphasis added).

33 The *bona fide* test was adopted by the Ontario Court of Appeal in *Straka v. Humber River Regional Hospital* (2000), 51 O.R. (3d) 1 (Ont. C.A.) where the respondent sought to compel production of confidential reference letters that had resulted in the respondent's failure to obtain an employment position. The Prince Edward Island Court of Appeal in *Johnston v. Frank Johnston's Restaurants Ltd.*, [1980] P.E.I.J. No. 34 (P.E.I. C.A.) also adopted the *bona fide* test in a situation where the plaintiffs claimed they did not know the identity of persons they wished to sue.

34 In my view, it would make little sense to require proof of a *prima facie* case at the stage of the present proceeding. The plaintiffs do not know the identity of the persons they wish to sue, let alone the details of precisely what was done by each of them such as to actually prove infringement. Such facts would only be established after examination for discovery and trial. The plaintiffs would be effectively stripped of a remedy if the Courts were to impose upon them, at this stage, the burden of showing

2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

a *prima facie* case. It is sufficient if they show a *bona fide* claim, i.e. that they really do intend to bring an action for infringement of copyright based upon the information they obtain, and that there is no other improper purpose for seeking the identity of these persons.

### Other Criteria relating to Equitable Bills of Discovery

35 As to the other criteria for granting an equitable bill of discovery, I agree with the conclusions of the Motions Judge. There should be clear evidence to the effect that the information cannot be obtained from another source such as the operators of the named websites (KaZaA, *et al*). Also if an order for disclosure were granted, consideration would have to be given to the costs incurred by the respondents in assembling the information.

### Privacy Issues

36 I agree with the Motions Judge's characterization of the 5<sup>th</sup> criteria - that is - the public interest in favour of disclosure must outweigh the legitimate privacy concerns of the person sought to be identified if a disclosure order is made.

37 All respondents raise the privacy issue. It is an important consideration. Pursuant to PIPEDA, ISPs are not entitled to "voluntarily" disclose personal information such as the identities requested except with the customer's consent or pursuant to a court order. Indeed, pursuant to subsections 7(3)(c), 8(8) and 28 of PIPEDA, any organization that receives a request for the release of personal information must "retain the information for as long as is necessary to allow the individual to exhaust any recourse" under PIPEDA. Failure to comply could result in the organization being found guilty of an offence punishable on summary conviction or an indictable offence.

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

...

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

...

8. (8) Despite clause 4.5 of Schedule 1, an organization that has personal information that is the subject of a request shall retain the information for as long as is necessary to allow the individual to exhaust any recourse under this Part that they may have.

...

28. Every person who knowingly contravenes subsection 8(8) or 27.1(1) or who obstructs the Commissioner or the Commissioner's delegate in the investigation of a complaint or in conducting an audit is guilty of

(a) an offence punishable on summary conviction and liable to a fine not exceeding \$10,000; or

7. (3) Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation ne peut communiquer de renseignement personnel à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

...

c) elle est exigée par assignation, mandat ou ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de documents;

...

8(8) Malgré l'article 4.5 de l'annexe 1, l'organisation qui détient un renseignement faisant l'objet d'une demande doit le conserver le temps nécessaire pour permettre au demandeur d'épuiser ses recours.

...

28. Quiconque contrevient sciemment aux paragraphes 8(8) ou 27.1(1) ou entrave l'action du commissaire -- ou de son délégué -- dans le cadre d'une vérification ou de l'examen d'une plainte commet une infraction et encourt, sur déclaration de culpabilité :

a) par procédure sommaire, une amende maximale de 10 000 \$;

2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

(b) an indictable offence and liable to a fine not exceeding \$100,000.

b) par mise en accusation, une amende maximale de 100 000 \$.

38 Privacy rights are significant and they must be protected. In order to achieve the appropriate balance between privacy rights and the public interest in favour of disclosure, PIPEDA provides protection over personal information that is collected, held and used by organizations and allows disclosure of such information only in certain circumstances, enumerated in subsection 7(3). The purpose of PIPEDA, which is the establishment of rules governing the "collection, use and disclosure of personal information", is articulated in section 3, which specifically states,

3. The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

3. La présente partie a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances.

39 The delicate balance between privacy interests and public interest has always been a concern of the court where confidential information is sought to be revealed. Although PIPEDA had not been enacted at the time of the *Glaxo* decision, Stone J.A. nonetheless noted at paragraph 62:

I am not persuaded that this is a sufficient justification for refusing to disclose the identity of the importers in the present case. While section 107 implies that information collected pursuant to the Act will be treated as confidential, section 108 indicates that it is susceptible to disclosure in certain situations. I am thus doubtful that importers have a high expectation of confidentiality regarding the information which they furnish to customs officials. More important, I am sceptical about the expectation and degree of confidentiality associated with the nature of the information which the appellant seeks. As the House of Lords observed in *Norwich Pharmacal*, *supra*, the names of the importers are likely to pass through many hands before reaching those of customs officials. It is therefore not reasonable to regard the identity of the importers as particularly sensitive information. In my opinion, in the circumstances of this case the public interest in ensuring that the appellant is able to pursue in the courts those who have allegedly violated its patent rights outweighs the public interest in maintaining the confidentiality of the importers' names.

He also approved, at paragraph 26, of the statement of Viscount Dilhorne in *Norwich* as follows:

Subject to the public interest in protecting the confidentiality of information given to Customs, in my opinion it is clearly in the public interest and right for protection of patent holders, where the validity of the patent is accepted and the infringement of it not disputed, that they should be able to obtain by discovery the names and addresses of the wrongdoers from someone involved but not a party to the wrongdoing.

40 The reasoning in *Glaxo* and *Norwich* is compelling. Intellectual property laws originated in order to protect the promulgation of ideas. Copyright law provides incentives for innovators - artists, musicians, inventors, writers, performers and marketers - to create. It is designed to ensure that ideas are expressed and developed instead of remaining dormant. Individuals need to be encouraged to develop their own talents and personal expression of artistic ideas, including music. If they are robbed of the fruits of their efforts, their incentive to express their ideas in tangible form is diminished.

41 Modern technology such as the Internet has provided extraordinary benefits for society, which include faster and more



2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

efficient means of communication to wider audiences. This technology must not be allowed to obliterate those personal property rights which society has deemed important. Although privacy concerns must also be considered, it seems to me that they must yield to public concerns for the protection of intellectual property rights in situations where infringement threatens to erode those rights.

42 Thus, in my view, in cases where plaintiffs show that they have a *bona fide* claim that unknown persons are infringing their copyright, they have a right to have the identity revealed for the purpose of bringing action. However, caution must be exercised by the courts in ordering such disclosure, to make sure that privacy rights are invaded in the most minimal way.

43 If there is a lengthy delay between the time the request for the identities is made by the plaintiffs and the time the plaintiffs collect their information, there is a risk that the information as to identity may be inaccurate. Apparently this is because an IP address may not be associated with the same individual for long periods of time. Therefore it is possible that the privacy rights of innocent persons would be infringed and legal proceedings against such persons would be without justification. Thus the greatest care should be taken to avoid delay between the investigation and the request for information. Failure to take such care might well justify a court in refusing to make a disclosure order.

44 Also, as the intervener, Canadian Internet Policy and Public Interest Clinic, pointed out, plaintiffs should be careful not to extract private information unrelated to copyright infringement, in their investigation. If private information irrelevant to the copyright issues is extracted, and disclosure of the user's identity is made, the recipient of the information may then be in possession of highly confidential information about the user. If this information is unrelated to copyright infringement, this would be an unjustified intrusion into the rights of the user and might well amount to a breach of PIPEDA by the ISPs, leaving them open to prosecution. Thus in situations where the plaintiffs have failed in their investigation to limit the acquisition of information to the copyright infringement issues, a court might well be justified in declining to grant an order for disclosure of the user's identity.

45 In any event, if a disclosure order is granted, specific directions should be given as to the type of information disclosed and the manner in which it can be used. In addition, it must be said that where there exists evidence of copyright infringement, privacy concerns may be met if the court orders that the user only be identified by initials, or makes a confidentiality order.

### Infringement of Copyright

46 As has been mentioned, the Motions Judge made a number of statements relating to what would or would not constitute infringement of copyright. (See para. 15(f)). Presumably he reached these conclusions because he felt that the plaintiff, in order to succeed in learning the identity of the users, must show a *prima facie* case of infringement.

47 In my view, conclusions such as these should not have been made in the very preliminary stages of this action. They would require a consideration of the evidence as well as the law applicable to such evidence after it has been properly adduced. Such hard conclusions at a preliminary stage can be damaging to the parties if a trial takes place and should be avoided.

48 The danger in reaching such conclusions at the preliminary stages of an action without the availability of evidence nor consideration of all applicable legal principles are obvious and I will give some examples.

49 When the Motions Judge stated that, under subsection 80(1) of the *Copyright Act*, R.S. 1985, c. C-42, "downloading a song for personal use does not amount to infringement," he gave no consideration to the possible application of subsection 80(2) and the circumstances in which the defence of "private use" will not be available, such as, *inter alia*, where the reproduction of a musical work embodied in a sound recording onto an audio recording medium is done for the sale, rental, distribution, communication by telecommunication or performance to the public.

80. (1) Subject to subsection (2), the act of reproducing all or any substantial part of

80. (1) Sous réserve du paragraphe (2), ne constitue pas une violation du droit d'auteur protégeant tant l'enreg-



2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

istrement sonore que l'oeuvre musicale ou la prestation d'une oeuvre musicale qui le constituent, le fait de reproduire pour usage privé l'intégralité ou toute partie importante de cet enregistrement sonore, de cette oeuvre ou de cette prestation sur un support audio.

- (a) a musical work embodied in a sound recording,
- (b) a performer's performance of a musical work embodied in a sound recording, or
- (c) a sound recording in which a musical work, or a performer's performance of a musical work, is embodied

onto an audio recording medium for the private use of the person who makes the copy does not constitute an infringement of the copyright in the musical work, the performer's performance or the sound recording.

(2) Subsection (1) does not apply if the act described in that subsection is done for the purpose of doing any of the following in relation to any of the things referred to in paragraphs (1)(a) to (c):

- (a) selling or renting out, or by way of trade exposing or offering for sale or rental;
- (b) distributing, whether or not for the purpose of trade;
- (c) communicating to the public by telecommunication;

...

(2) Le paragraphe (1) ne s'applique pas à la reproduction de l'intégralité ou de toute partie importante d'un enregistrement sonore, ou de l'oeuvre musicale ou de la prestation d'une oeuvre musicale qui le constituent, sur un support audio pour les usages suivants :

- a) vente ou location, ou exposition commerciale;
- b) distribution dans un but commercial ou non;
- c) communication au public par télécommunication;

...

50 The Motions Judge also did not appear to consider whether all the requirements for the application of the exemption relating to personal use contained in subsection 80(1) of the *Copyright Act* were satisfied. For example, if the users were not using an "audio recording medium", the defence of private copying would not be available. (See *Copyright Board, Private copying 2003-2004* (December 12, 2003) and *Canadian Private Copying Collective v. Canadian Storage Media Alliance*, 2004 FCA 424 (F.C.A.).)

51 The Motions Judge relied upon the case of *CCH Canadian Ltd. v. Law Society of Upper Canada*, 2004 SCC 13 (S.C.C.) to say that there is no "authorization" by the users of the plaintiffs' sound recordings in the present case, when he had at the same time said the evidence as to infringement was inadequate. Obviously, at the early stages of this case, it is premature to reach any conclusion as to the applicability of the *CCH* case. Nor did the Motions Judge consider whether the users' act of copying the Songs onto their shared directory could constitute authorization because it invited and permitted other persons with Internet access to have the musical works communicated to them and be copied by them.

52 The Motions Judge similarly made findings that there had been no "distribution" within the meaning of the *Copyright Act* so as to constitute infringement. He said that to have distribution, there must be a "positive act by the owner of the shared directory", implying that making copies "available on their shared drives" is not a positive act. It is not clear that the legislation requires a "positive act" and no authority is cited in support of his conclusion.

53 The Motions Judge found no evidence of secondary infringement contrary to subsection 27(2) of the *Copyright Act* because there was "no evidence of knowledge on the part of the infringer." This ignores the possibility of finding infringement even without the infringer's actual knowledge, if indeed he or she "should have known" there would be infringement. *Copyright Act* subsection 27(2):

2005 CarswellNat 1300, 2005 FCA 193, 39 C.P.R. (4th) 97, 252 D.L.R. (4th) 342, 334 N.R. 268, [2005] 4 F.C.R. 81

(2) It is an infringement of copyright for any person to

(2) Constitue une violation du droit d'auteur l'accomplissement de tout acte ci-après en ce qui a trait à l'exemplaire d'une oeuvre, d'une fixation d'une prestation, d'un enregistrement sonore ou d'une fixation d'un signal de communication alors que la personne qui accomplit l'acte sait ou devrait savoir que la production de l'exemplaire constitue une violation de ce droit, ou en constituerait une si l'exemplaire avait été produit au Canada par la personne qui l'a produit:

...

(b) distribute to such an extent as to affect prejudicially the owner of the copyright,

...

b) la mise en circulation de façon à porter préjudice au titulaire du droit d'auteur;

...

(d) possess for the purpose of doing anything referred to in paragraphs (a) to (c)...

...

d) la possession en vue de l'un ou l'autre des actes visés aux alinéas a) à c); (je souligne)

a copy of a work, sound recording or fixation of a performer's performance or of a communication signal that the person knows or should have known infringes copyright or would infringe copyright if it had been made in Canada by the person who made it. (emphasis added)

54 Thus, the danger of making such findings at the early stages of this case can be seen. I make no such findings here and wish to make it clear that if this case proceeds further, it should be done on the basis that no findings to date on the issue of infringement have been made.

55 In the result, the appeal will be dismissed without prejudice to the plaintiffs' right to commence a further application for disclosure of the identity of the "users" taking into account these reasons.

56 Having regard to what must be considered as divided success on this appeal, there will be no order as to costs.

**Richard C.J.:**

I agree

**Noël J.A.:**

I agree

*Appeal dismissed.*

END OF DOCUMENT

2011 CarswellNat 4129, 2011 FC 1024, 2011 CF 1024, 395 F.T.R. 315 (Eng.)

2011 CarswellNat 4129, 2011 FC 1024, 2011 CF 1024, 395 F.T.R. 315 (Eng.)

Voltages Pictures LLC c. Untel

Voltages Pictures LLC, Plaintiff and Jane Doe and John Doe, Defendants

Federal Court

Michel M.J. Shore J.

Heard: August 29, 2011  
Judgment: August 29, 2011  
Docket: T-1373-1

© Thomson Reuters Canada Limited or its Licensors (excluding individual court documents). All rights reserved.

Counsel: Greg Moore, for Plaintiff

No one for Defendant

Subject: Civil Practice and Procedure

Civil practice and procedure.

***Michel M.J. Shore J.:***

[UNREVISED ENGLISH CERTIFIED TRANSLATION]

## **I. Preliminary**

1 A copyright infringement gives rise to extraordinary measures in order to find the parties guilty of that infringement.

## **II. Introduction**

2 In *BMG Canada Inc. v. John Doe*, 2005 FCA 193, [2005] 4 F.C.R. 81, the Federal Court of Appeal confirmed the following:

[42] ... in cases where plaintiffs show that they have a *bona fide* claim that unknown persons are infringing their copyright, they have a right to have the identity revealed for the purpose of bringing action....

2011 CarswellNat 4129, 2011 FC 1024, 2011 CF 1024, 395 F.T.R. 315 (Eng.)

3 The Court accepts the plaintiff's position in support of its motion as follows:

(i) an order allowing for a written examination for discovery of Bell Canada, Cogeco Cable Inc. and Videotron GP to be held so that they identify the names and addresses connected to their customer accounts associated with the IP addresses at the times specified in Annex A of the Statement of Claim filed in this record; and

(ii) an order requiring Bell Canada, Cogeco Cable Inc. and Videotron GP to disclose to Voltage Pictures LLC the names and addresses related to their customer accounts associated with the IP addresses at the times specified in Annex A of the Statement of Claim filed in this record.

4 Voltage Pictures LLC is the owner of the copyright on the film *Hurt Locker*. The defendants copied and distributed this film over the internet without the authorization of Voltage Pictures LLC.

5 Voltage Pictures LLC has identified the IP addresses used by the defendants, but only their internet service providers can identify them more precisely.

6 Voltage Pictures LLC is seeking leave to conduct a written examination for discovery of the internet service providers so that they disclose the names and addresses of the customers corresponding to the IP addresses already obtained. Once these customers have been identified, Voltage Pictures LLC can send formal notices and, where applicable, add these persons as defendants to this action.

### III. Facts

7 The defendants downloaded, copied and distributed the film *Hurt Locker* through peer-to-peer networks on the internet, without the authorization of Voltage Pictures LLC. They did so anonymously; they can be identified only by their IP addresses (Affidavit of Daniel Arheidt, sworn on August 24, 2011, at paras. 23-25).

8 An IP address is merely a series of numbers, as appears from the table attached as Annex A to the Statement of Claim dated June 20, 2011.

9 The IP addresses in question belong to Bell Canada, Cogeco Cable Inc. and Videotron GP (internet service providers) and are used by customers when they access the internet. The internet service providers record the use of their IP addresses and can identify who has used an IP address at a specific time and date (Affidavit of Daniel Arheidt at para 23).

10 Voltage Pictures LLC must therefore call upon the internet service providers to obtain the names and addresses corresponding to the IP addresses that it has already obtained by consulting public sources.

11 Without this information, Voltage Pictures LLC cannot identify those persons who have infringed its copyright and will be deprived of its right to bring an action against them.

### IV. Analysis

#### ***Subsection 7(3) of the Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5***

12 Voltage Pictures LLC is asking the internet service providers to disclose the names and addresses of some of their customers who have allegedly infringed its copyright.

13 Subsection 7(3) of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, allows

2011 CarswellNat 4129, 2011 FC 1024, 2011 CF 1024, 395 F.T.R. 315 (Eng.)

for the disclosure of personal information on a court order:

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

...

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

7. (3) Pour l'application de l'article 4.3 de l'annexe 1 et malgré la note afférente, l'organisation ne peut communiquer de renseignement personnel à l'insu de l'intéressé et sans son consentement que dans les cas suivants:

[...]

c) elle est exigée par assignation, mandat ou ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de documents;

14 *According to the Federal Court of Appeal, a written examination for discovery of the internet service providers is appropriate where their customers have infringed the plaintiff's copyright:*

[25] However, the appellants argued that the main issue on the motion was the identity of each person who is committing infringement of the appellants' copyrights. I agree and find that because this issue inevitably falls within the words in subsection 238(1) of the Rules as being "an issue in the action," rule 238 is broad enough to permit discovery in cases such as this.

...

[41] Modern technology such as the Internet has provided extraordinary benefits for society, which include faster and more efficient means of communication to wider audiences. This technology must not be allowed to obliterate those personal property rights which society has deemed important. Although privacy concerns must also be considered, it seems to me that they must yield to public concerns for the protection of intellectual property rights in situations where infringement threatens to erode those rights.

[42] Thus, in my view, in cases where plaintiffs show that they have a *bona fide* claim that unknown persons are infringing their copyright, they have a right to have the identity revealed for the purpose of bringing action. However, caution must be exercised by the courts in ordering such disclosure, to make sure that privacy rights are invaded in the most minimal way.

(BMG, above)

15 These principles also apply to the case at bar.

***Rule 238 of the Federal Courts Rules, SOR/98-106***

16 To obtain the name and address of a customer of an internet service provider, plaintiffs must prove that they

2011 CarswellNat 4129, 2011 FC 1024, 2011 CF 1024, 395 F.T.R. 315 (Eng.)

have a *bona fide* claim against that customer and that they meet the criteria of Rule 238 of the *Federal Courts Rules* (BMG, above, at paras. 33 and 34).

17 Voltage Pictures LLC has a *bona fide* claim against the defendants: it has brought an action against them for having infringed its copyright when they copied and publicly distributed the film *Hurt Locker*.

18 Rule 238 of the *Federal Courts Rules* allows for the holding of an examination for discovery of a third party where the third party has relevant information on an issue in the action:

**238. (1)** A party to an action may bring a motion for leave to examine for discovery any person not a party to the action, other than an expert witness for a party, who might have information on an issue in the action.

...

(3) The Court may, on a motion under subsection (1), grant leave to examine a person and determine the time and manner of conducting the examination, if it is satisfied that

- (a) the person may have information on an issue in the action;
- (b) the party has been unable to obtain the information informally from the person or from another source by any other reasonable means;
- (c) it would be unfair not to allow the party an opportunity to question the person before trial; and
- (d) the questioning will not cause undue delay, inconvenience or expense to the person or to the other parties.

**238. (1)** Une partie à une action peut, par voie de requête, demander l'autorisation de procéder à l'interrogatoire préalable d'une personne qui n'est pas une partie, autre qu'un témoin expert d'une partie, qui pourrait posséder des renseignements sur une question litigieuse soulevée dans l'action.

[...]

(3) Par suite de la requête visée au paragraphe (1), la Cour peut autoriser la partie à interroger une personne et fixer la date et l'heure de l'interrogatoire et la façon de procéder, si elle est convaincue, à la fois:

- a) que la personne peut posséder des renseignements sur une question litigieuse soulevée dans l'action;
- b) que la partie n'a pu obtenir ces renseignements de la personne de façon informelle ou d'une autre source par des moyens raisonnables;
- c) qu'il serait injuste de ne pas permettre à la partie d'interroger la personne avant l'instruction;
- d) que l'interrogatoire n'occasionnera pas de retards, d'inconvénients ou de frais déraisonnables à la personne ou aux parties.

19 These criteria are factual and are assessed on a case-by-case basis.

**Paragraph 238(3)(a) of the Federal Courts Rules — the internet service providers have relevant information**



2011 CarswellNat 4129, 2011 FC 1024, 2011 CF 1024, 395 F.T.R. 315 (Eng.)

20 Voltage Pictures LLC does not know the names and addresses of the defendants. Since they are all customers of the internet service providers, the internet service providers can match the IP addresses identified by Voltage Pictures LLC with their internal records and provide the names and addresses of the defendants.

21 This information is, in fact, relevant to this case.

***Paragraph 238(3)(b) of the Federal Courts Rules — Voltage Pictures LLC has been unable to obtain this information informally***

22 The internet service providers cannot disclose the names and address of their customers without an order of this Court.

***Paragraph 238(3)(c) of the Federal Courts Rules — it would be unfair not to allow Voltage Pictures LLC an opportunity to question the internet service providers***

23 In *BMG*, above, the Federal Court of Appeal confirmed:

[42] ... in cases where plaintiffs show that they have a *bona fide* claim that unknown persons are infringing their copyright, they have a right to have the identity revealed for the purpose of bringing action...

24 Voltage Pictures LLC cannot assert its copyright or bring an action against the defendants if it does not know their names and addresses.

25 Defendants should not have the possibility of hiding behind the anonymity of the internet and continuing to infringe the copyright of Voltage Pictures LLC.

***Paragraph 238(3)(d) of the Federal Courts Rules — the questioning will not cause undue delay, inconvenience or expense to the person or to the other parties***

26 Voltage Pictures LLC agrees to reimburse any reasonable expenses incurred by the internet service providers in collecting the information sought.

27 Obtaining the names and addresses of the defendants will speed up this action. Without this information, Voltage Pictures LLC cannot assert its rights.

28 Voltage Pictures LLC is asking this Court that the minimum information necessary to allow it to assert its rights against the defendants be disclosed to it.

#### **IV. Conclusion**

29 The Court grants Voltage Pictures LLC's motion without costs given that the plaintiff's motion is not contested by any of the internet service providers.

#### **Judgment**

Further to the analysis undertaken, *the Court orders that:*

2011 CarswellNat 4129, 2011 FC 1024, 2011 CF 1024, 395 F.T.R. 315 (Eng.)

1. Voltage Pictures LLC proceed with a written examination for discovery of Bell Canada, Cogeco Cable Inc. and Videotron GP in order to obtain the names and addresses related to their customer accounts associated with the IP addresses at the times specified in Annex A attached to the Notice of Motion.
2. Within two weeks, Bell Canada, Cogeco Cable Inc. and Videotron GP disclose to Voltage Pictures LLC the names and addresses related to their customer accounts associated with the IP addresses at the times specified in Annex A. This disclosure shall be in Microsoft Excel format, with publishing rights, encrypted on a compact disk or any other electronic medium.
3. Voltage Pictures LLC reimburse any reasonable expenses incurred by Bell Canada, Cogeco Cable Inc. and Videotron GP in collecting the personal information identified in paragraph 1 of this order.
4. Without costs.

END OF DOCUMENT



2009 CarswellOnt 8689,

2009 CarswellOnt 8689

R. v. Brzezinski

R. v. Louis Brzezinski

Ontario Superior Court of Justice

A.W. Bryant J.

Heard: October 2, 2009

Judgment: November 27, 2009

Docket: 00003/09

© Thomson Reuters Canada Limited or its Licensors (excluding individual court documents). All rights reserved.

Counsel: Jennifer Gleitman for Crown / Respondent

David Humphrey for Applicant, Louis Brzezinski

Subject: Criminal; Evidence

Criminal law --- Pre-trial procedure — Search with warrant — Information — Substantive requirements — Reasonable and probable grounds.

Evidence --- Opinion — Experts — Hypothetical questions.

**Cases considered by A.W. Bryant J.:**

*R. v. Abadom* (1982), 76 Cr. App. R. 48, [1983] 1 All E.R. 364, [1983] 1 W.L.R. 126 (Eng. C.A.) — referred to

*R. v. Araujo* (2000), [2000] 2 S.C.R. 992, 79 C.R.R. (2d) 1, 2000 SCC 65, 2000 CarswellBC 2438, 2000 CarswellBC 2440, 38 C.R. (5th) 307, 193 D.L.R. (4th) 440, 149 C.C.C. (3d) 449, 143 B.C.A.C. 257, 235 W.A.C. 257, 262 N.R. 346 (S.C.C.) — followed

*R. v. Corbett* (1988), [1988] 1 S.C.R. 670, [1988] 4 W.W.R. 481, 85 N.R. 81, 28 B.C.L.R. (2d) 145, 41 C.C.C. (3d) 385, 64 C.R. (3d) 1, 34 C.R.R. 54, 1988 CarswellBC 756, 1988 CarswellBC 252 (S.C.C.) — referred to

*R. v. Garofoli* (1990), 80 C.R. (3d) 317, [1990] 2 S.C.R. 1421, 116 N.R. 241, 43 O.A.C. 1, 36 Q.A.C. 161, 60 C.C.C. (3d) 161, 50 C.R.R. 206, 1990 CarswellOnt 119, 1990 CarswellOnt 1006 (S.C.C.) — followed

*R. v. Grandinetti* (2005), 37 Alta. L.R. (4th) 197, 329 N.R. 28, [2005] 1 S.C.R. 27, 247 D.L.R. (4th) 385, 25 C.R. (6th) 1, 191 C.C.C. (3d) 449, [2005] 4 W.W.R. 405, 2005 CarswellAlta 81, 2005 CarswellAlta 82, 2005 SCC 5, 363 A.R. 1, 343 W.A.C. 1 (S.C.C.) — considered

2009 CarswellOnt 8689,

*R. v. Morrissey* (1995), 1995 CarswellOnt 18, 38 C.R. (4th) 4, 22 O.R. (3d) 514, 97 C.C.C. (3d) 193, 80 O.A.C. 161 (Ont. C.A.) — considered

*R. v. Terceira* (1998), 38 O.R. (3d) 175, 15 C.R. (5th) 359, 1998 CarswellOnt 390, 107 O.A.C. 15, 123 C.C.C. (3d) 1 (Ont. C.A.) — referred to

*R. v. Terceira* (1999), 1999 CarswellOnt 4027, 1999 CarswellOnt 4028, [1999] 3 S.C.R. 866, 142 C.C.C. (3d) 95, 32 C.R. (5th) 77, 46 O.R. (3d) 96, 129 O.A.C. 283, 250 N.R. 98 (S.C.C.) — referred to

*R. v. Watson* (1996), 1996 CarswellOnt 2884, 108 C.C.C. (3d) 310, 50 C.R. (4th) 245, 92 O.A.C. 131, 30 O.R. (3d) 161 (Ont. C.A.) — considered

#### **Statutes considered:**

*Criminal Code*, R.S.C. 1985, c. C-46

Generally — referred to

s. 163.1(1) "child pornography" [en. 1993, c. 46, s. 2] — referred to

s. 487 — considered

#### **Forms considered:**

*Criminal Code*, R.S.C. 1985, c. C-46

Form 1 — referred to

#### ***A.W. Bryant J.:***

1 On March 24, 2009, Justice of the Peace C.J. Dube, at the Town of Markham, issued a search warrant to peace officers in the municipality of York Region, authorizing them to search a dwelling house located at 30 Gordon Rowe Crescent, Richmond Hill, Ontario for evidence in respect of the commission or suspected commission of possessing and making available child pornography between January 6, 2009 and March 22, 2009. The applicant, Mr. Louis Brzezinski, brought an application in the nature of certiorari to quash the warrant.

#### **I. Grounds for the Application**

2 The notice of application set out the following grounds:

1. that the search warrant was issued upon an information which failed to disclose the required reasonable grounds to justify the issuance of a search warrant;
2. that the Information to Obtain the search warrant failed to disclose any information respecting the existence, or non-existence, of a wireless network associated with the computer(s) associated with the suspect Internet Protocol ("IP") address, and failed to disclose whether any investigation had been done by the police to ascertain the existence, or non-existence, of such network;

2009 CarswellOnt 8689,

3. that had the issuing Justice been made aware of the possible existence of an unsecured wireless network associated with the suspect IP address, there would have been no reasonable grounds to search the residence of the subscriber of the suspect IP address by any number of other people using computers in other residences in the neighbourhood over an unsecured wireless network;

4. that in respect of the affiant downloading four files on March 18, 2009, the Information to Obtain does not set out how the computer associated with the suspect IP address was accessed by the affiant on that occasion and how the four files were downloaded on that occasion; and,

5. that the search warrant was executed by the York Region Police on the residence of the Applicant at 30 Gordon Rowe Crescent, Richmond Hill, Ontario on March 25, 2009.

## **II. Information to Obtain - Use of the Internet for Downloading and Sharing Child Pornography**

3 Detective Chris Barrie, the affiant, has been a police officer for 22 years. He is currently a member of the Internet Child Exploitation Unit of the York Regional Police. The unit investigates the manufacture, distribution, sale, importation and possession of child pornography. Since October 2006, he has been involved in child pornography investigations and received training on electronic investigative techniques concerning the distribution of child pornography on the internet.

4 Detective Barrie was the affiant to obtain the search warrant for a dwelling house located at 30 Gordon Crowe Crescent, Richmond Hill Ontario ("target residence"). In the Information to Obtain a search warrant, Detective Barrie stated that child pornography in the form of computer generated graphics, images and compressed movies are capable of being viewed and stored on a computer. An image, photograph or movie found on a computer can be processed to generate a unique identifying data (called a "hash value") for that digitized image, photograph or video. A new "hash value" is generated whenever any change is made to a computer file.

5 Detective Barrie stated that there are open source public file sharing networks ("peer to peer" networks) which are used to trade, share or distribute child pornography. Also, there are computer programs which allow a person to access these networks to share computer files. In addition, some persons ("ultra peers") maintain an index of pornographic computer files and each file has a unique digital identifier regardless of the file names. When a user searches the internet to download a pornographic computer file of an image, photograph or video, the index informs the user where the file (as identified by its unique digital identifier) is available for downloading. The user searches on the internet for the computer offering to share that pornographic image, photograph or video and saves a copy on his own computer. Since these transactions occur on the internet, the police using special investigative techniques are able to detect and investigate the IP internet address of those computers involved in sharing known pornographic digital files.

6 Detective Barrie is able to identify IP addresses that are likely in York Region containing suspected child pornography and to generate a historic report showing the dates and times that a computer at a particular IP address was logged on to the file sharing network and the digital identifier of suspected child pornographic images, photographs or videos that were available for sharing.

7 The warrant authorized Detective Barrie to search for and seize computer system(s), devices capable of storing computer data, photographs, videos and computer files which show either a person who is or is depicted as being under 18 years old who is engaged in or depicted as being engaged in explicit sexual activity or the dominant characteristic of which is the depiction for sexual purpose of a sexual organ or the anal region of a person under the age of eighteen years old. The warrant authorized Detective Barrie to search for computer files or documentation for evidence concerning the identity the owner or a person(s) who controls the computer system(s) or the pornographic data.

2009 CarswellOnt 8689,

8 On February 23, 2009, Detective Barrie was monitoring public file sharing networks to determine if any persons offered to share child pornography. He observed that a computer at IP address 99.238.115.78 (the "target IP address") had files which were available to the public that contained suspected child pornography. Detective Barrie further determined that the target IP address appeared to be located in York Region. Detective Barrie attempted to browse the shared folder of the target IP address but was unable to do so.

9 On February 23, 2009, Detective Barrie prepared an IP history report for the target IP address. The report indicated that the target IP address had suspected child pornography files available for downloading by the general public on 316 occasions between January 6, 2009 and February 22, 2009. The title of ten suspect files indicated they contained child pornography, for example, "9 yo Vicky stripping and sucking (kiddy pedo illegal underage preteen)."

10 Detective Barrie used an electronic investigative tool to determine that Rogers Communications Inc. was the Internet Service Provider ("ISP") for the targeted IP address. He did not know if the target IP address received internet service through a wireless router.

11 On March 17, 2009, he requested Rogers Communications to inform him of the identity of the account holder of the target internet address for the period January 6, 2009 and February 22, 2009. On the same date, he learned the subscriber was L. Brzezinski, at 30 Richmond Hill Crescent and it was an active internet account. Later that day, he drove past 30 Richmond Hill Drive and observed it was a two story detached house.

12 Detective Barrie obtained background information on Mr. Brzezinski and 30 Richmond Hill Crescent. A Ministry of Transportation search conducted on March 17, 2009 revealed that Louis Brzezinski had a driver's licence and resided at 30 Gordon Rowe Crescent. A search of a police data base revealed that Marcie Weiman was ticketed driving a motor vehicle registered to Louis Brzezinski. He attended at the Richmond Hill Tax Office on March 18, 2009 and learned that the owners of 30 Gordon Rowe Crescent were Louis Brzezinski and Marcie Weiman.

13 On March 19, 2009, a York Region police officer observed vehicles at the target residence confirming Louis Brzezinski was the owner of the residence. On March 23, 2009, a member of the York Region police conducted an on line search and determined that an individual by the name of Jack Brzezinski likely also resides at the target address. It was further learned that an individual named Louis Brzezinski had a law office in Toronto and practiced civil law.

14 On March 18, 2009, Detective Barrie downloaded four files with the same "hash values" that the target IP address previously made available for downloading. These copies of the four files were obtained through another source.

15 On March 23, 2009, Detective Barrie viewed the content of these four files and described what was depicted on the videos. The first video was described as: "a compilation of several videos depicting pre-pubescent girls involved in oral sex with unknown males. In several of the video's the male is observed ejaculating on the girls." He described the content of the other three videos as depicting bondage and oral sex, anal and vaginal penetration by males with pre-pubescent girls. Detective Barrie formed the opinion that these videos were consistent with the *Criminal Code*, R.S.C. 1985, c. C-46, definition of child pornography.

16 On the same date, Detective Barrie prepared a fresh IP history for the target IP address. The report showed that the IP address broadcasted as a download candidate for suspected child pornography on 515 occasions between January 6, 2009 and March 22, 2009.

17 On March 24, 2009, Detective Barrie applied for a search warrant. No further investigative steps were referred to in the Information to Obtain.

18 On March 25, 2009, a search warrant was executed. The police seized electronic equipment including com-

2009 CarswellOnt 8689,

puter(s) and storage devices. The items seized were immediately segregated and have not been searched pending an order of the court regarding a claim for solicitor client privilege.

### III. Evidence on the Application

19 Counsel agreed that Detective Barrie and Martin Musters, a computer expert, would be called as witnesses on the application.

20 Mr. Musters was qualified to give opinion evidence as to whether the existence, or possible existence, of a wireless network at the IP address associated with the Applicant's home address would assist in determining whether the downloading or sharing of electronic data was being done from the Applicant's home or from some other location.

21 Mr. Muster opined that wireless networks are commonly used in residences to allow access to the internet without the necessity of physically connecting a computer to a cable or phone line. It was his evidence that most computers currently on the market today are equipped with a wireless card and can access wireless networks.

22 It was Mr. Muster's evidence that wireless networks typically have a range of 150 feet indoors and 300 feet outdoors. He testified that a wireless router located close a window would have a range of approximately 225 feet. He said that 30 Gordon Rowe Crescent is located in a residential area. The lots are approximately 50 feet wide by 100 feet deep and ten houses are within approximately 225 feet of the target residence: three houses to the south (across the street), two houses to the east, two houses to the west and three houses to the north (behind 30 Gordon Rowe Crescent). He opined that up to eleven different residences and any mobile computer within a 225 foot radius were capable of accessing a wireless network located inside the target residence. Further, any person who accessed the internet through a wireless network originating from 30 Gordon Rowe Crescent would be doing so through the target IP address.

23 In the summer of 2009, he conducted a search on his laptop computer for wireless networks while parked in his vehicle outside 30 Gordon Rowe Crescent. He detected five wireless networks, two of which were not secured by a password. Detective Barrie confirmed that wireless networks existed and some of them were not secured.

24 Mr. Musters testified that police can identify the IP address which is downloading or sharing files from a file sharing network but the police cannot identify the specific computer the files are being shared from or downloaded. In his affidavit filed on the application he stated: "While it is possible to determine the IP address to which files are being downloaded or from which files are being shared, it is impossible to determine, without access to the individual computers, which computer within a wireless network for a particular IP address is being used for this activity."

25 Mr. Munster informed the Court that wireless networks are either secure (password protected) or unsecured. He estimated that sixty percent of wireless networks are secure. It was his evidence that even if a wireless network is secured, access to the network can be gained if the password has been shared or otherwise obtained until such time as the password for the router is changed.

26 Mr. Munster opined that the police could detect whether a wireless network is present at a particular address by viewing available wireless networks on a laptop while situated outside of the target residence. If multiple networks are present, police should be able to determine which network is associated with a target address by examining the signal strength of the different networks. He agreed in cross-examination that factors such as location within a residence may affect signal strength.

27 Detective Barrie testified that in several previous investigations he attempted to link wireless networks to a specific address by signal strength. It was his experience that signal strength was not reliable to link a wireless address to a computer.



2009 CarswellOnt 8689,

28 Detective Barrie testified that he did not have the ability to electronically investigate whether there was an unsecured router was at a particular residence unless he first obtained a judicial authorization under the *Criminal Code*. It was his evidence that the police technician might be able to determine which computer(s) was using a router at a target address by conducting electronic tests once the police had seized the router.

29 Detective Barrie testified that he needed to examine the electronic equipment to determine if the photographic images and videos were located at 30 Gordon Rowe Crescent. The technical analysis of the data is pending the resolution of the solicitor client procedures.

30 Detective Barrie did not investigate whether or not the target IP was a wireless network or inform the justice of the peace about wireless networks. He agreed that third parties could access a target IP address through an unsecured wireless network. He agreed that it is possible to detect wireless access in an area but he is not able to identify the residence it is connected to unless the network identifies itself by name or address.

31 It was Detective Barrie's evidence that signal strength of a wireless network does not assist determining the location of a router and that signal strength was not a reliable test to identify a target residence.

32 It was his view that the existence or non-existence of a wireless network at 30 Gordon Crescent was not important because the information obtained from the seized computer systems and storage units would assist his investigation of the listed offences. He said that the neighbours would be eliminated as suspects if there was not a wireless network at the Brzezinski residence. The police needed to investigate whether there was pornographic data at the target address even if there was an unsecured wireless network at the Brzezinski household. If pornographic material was not found at the Brzezinski the police needed to examine the router to identify the third party who used the target IP address as a download candidate.

#### **IV. Position of the Parties**

33 It is the applicant's position that Detective Barrie should have disclosed to the justice of the peace that there was a possibility that the applicant had an unsecured wireless network. Counsel argued that the presence of a wireless network would affect whether or not there were grounds to believe that evidence of the offence would be found at the target residence.

34 The applicant further submitted that if there was an unsecured wireless network at 30 Gordon Crescent then ten of surrounding residences were equally capable of engaging in the illegal activity and that the pornographic images, photographs or videos will be found in the residence of a neighbour. The applicant submitted that Detective Barrie should have investigated whether it was an unsecured wireless network associated with the Brzezinski residence.

35 It is the respondent's position that that the investigative steps followed by Detective Barrie as outlined in the Information to Obtain provided reasonable and probable grounds to believe a criminal offence had been committed and that evidence of the offence would be found at Mr. Brzezinski's residence.

36 Crown counsel submitted that the investigating officer's experience that signal strength was not a reliable method to determine if there was a wireless network at the Brzezinski residence. Crown counsel submitted that police access to the router as suggested by Mr. Muster in his affidavit required a judicial authorization. Counsel further submitted that the suggestion by applicant's counsel to limit the initial warrant to a seizure of the router would likely lead to the destruction of evidence by the suspect.

#### **V. Analysis and Decision**

2009 CarswellOnt 8689,

37 Section 487 of the *Criminal Code* requires any information on oath in Form 1 to be presented to a justice of the peace. The justice of the peace must be satisfied that there are reasonable and probable grounds to believe that there is in a building ... anything that there are reasonable grounds to believe will afford evidence with respect to the commission, suspected commission or intended commission of an offence.

38 Counsel for the applicant properly conceded that there were grounds to believe that an offence had been committed. Counsel focused his submissions on two issues: (1) there was a "real possibility" that there was an unsecured wireless network at the target residence and a neighbour used the target IP address for sharing and downloading computer files of pornographic images, photographs and videos; and, (2) the affiant should have informed the justice of the peace of the possibility of an unsecured wireless network at the target residence and that this possibility "fundamentally affects" whether or not there are grounds to believe that evidence of the offence will be found at the target residence.

***(a) The possible existence of an unsecured wireless network at the target residence***

39 Counsel for the applicant did not tender a witness who had first hand knowledge whether there was a wireless network at 30 Gordon Crescent or the age of the computer(s) in the residence. Mr. Munster, an expert, testified that virtually all laptop computers on the market today are equipped with a wireless card and can access wireless networks. Mr. Munster had no knowledge whether there was an unsecured wireless network at the Brzezinski residence between January 6, 2009 and March 22, 2009.

40 An exchange between counsel for the applicant and the Court occurred during oral argument:

The Court: So basically your position is that you have - have to eliminate - you have to assume that 30 Gordon Rowe Crescent was unsecured and you have to then go on and say you have to eliminate all the other possibilities before you can get a warrant?

Mr. Humphrey: Not all other possibilities.

The Court: Well...

Mr. Humphrey: You - you have to investigate to the point that you can say, based on all our investigation, we're at the point where there is a credibly based probability that it's at this house as opposed to the others. And again, if they'd gone outside and seen no networks, they're there. If they'd gone outside and - and- or used the word (ph) technique, if I can put it that way - if they'd investigated and satisfied themselves that there was a network but it was secured again -they'd have sufficient grounds.

The Court: But what - what's the basis that your - that your client had an unsecured network?

Mr. Humphrey: It's a - on the...

The Court: Are you just depending on the - on probability statistics?

Mr. Humphrey: Absolutely. It's very common. If this was some very, very remote possibility we wouldn't be before Your Honour on this motion making this argument...

The Court: Well, it's...

2009 CarswellOnt 8689,

Mr. Humphrey: ...and I won't repeat myself, but that's not where we are. Even in 2009, there were a lot of unsecured wireless networks...

The Court: I'm not talking about that, but it's all based on certain hypotheticals.

Mr. Humphrey: On - on possibilities. That's right

The Court: Hypothetical possibilities.

Mr. Humphrey: Right.

41 Counsel informed the Court that the grounds for quashing a warrant on this basis had not been previously judicially considered so I will examine the issue from first principles. In *R. v. Watson*, 50 C.R. (4th) 245, [1996] O.J. No. 2695 (Ont. C.A.) at para. 33, Doherty J.A. stated:

Relevance as explained in these authorities requires a determination of whether as a matter of human experience and logic the existence of 'Fact A' makes the existence or non-existence of 'Fact B' more probable than it would be without the existence of 'Fact A'. If it does then 'Fact A' is relevant to 'Fact B'.

There is no minimum value required in order for evidence to be deemed relevant (*R. v. Corbett*, [1988] 1 S.C.R. 670 (S.C.C.), at 715).

42 In the scenario proffered by the applicant, Fact A is the existence of an unsecured wireless network and Fact B is the possibility that a neighbour shared or downloaded pornographic data using the target IP address.

43 In *R. v. Morrissey*, [1995] O.J. No. 639 (Ont. C.A.) at para. 52, (1995), 22 O.R. (3d) 514 (Ont. C.A.), Doherty J.A. said:

A trier of fact may draw factual inferences from the evidence. The inferences must, however, be ones which can be reasonably and logically drawn from a fact or group of facts established by the evidence. An inference which does not flow logically and reasonably from established facts cannot be made and is condemned as conjecture and speculation.

44 It was Mr. Munster's opinion that it was possible for an unknown person in a nearby residence to connect to the target IP address through an unsecured wireless network at the Brzezinski residence and share or download pornographic data using the targeted IP. The proffered hypothesis could only occur if there was an unsecured wireless network at the target IP address.

45 Mr. Munster did not have first hand knowledge that (1) there was a wireless network at the Brzezinski residence; or, (2) the hypothetical Brzezinski wireless network was unsecured. The applicant's proposed hypothesis that a neighbour shared or downloaded the pornographic images was based upon Mr. Munster's anecdotal evidence that most computers on the market today have a wireless card and forty percent of wireless networks are unsecured.[FN1] As mentioned, there was no evidence of the age of the computer(s) at the Brzezinski residence.

46 It is my view that the required inference that a neighbour was the person who shared or downloaded pornographic data through a wireless connection cannot logically be drawn because the existence of a wireless network at the target IP has not been established by the evidence.

47 In *R. v. Grandinetti*, [2005] S.C.J. No. 3, 2005 SCC 5 (S.C.C.), the Supreme Court of Canada considered the



2009 CarswellOnt 8689,

threshold for the admissibility of evidence of the possible involvement of a third party in the commission of a specified offence. The Court articulated the following evidentiary threshold at para. 40:

The requirement that there be a sufficient connection between the third party and the crime is essential. Without this link, the third party evidence is neither relevant nor probative. The evidence may be inferential, but the evidence must be reasonable, based on the evidence, and not amount to speculation.

48 The only evidence that a third party neighbour might have connected to the target IP address to share or download pornographic data is Mr. Munster's opinion that it is a possibility. I find that the hypothetical possibility that another person might use the target IP address does not satisfy the requirement of a sufficient connection between the proffered third party and the crime.

49 I dismiss the application in the nature of certiorari to quash the search warrant based on the hypothetical possibility that a neighbour shared and downloaded pornographic data using the target IP address.

***(b) The Failure to disclose information to the Justice of the Peace***

50 Counsel for the applicant submitted that the Information to Obtain failed to disclose to Justice of the Peace Dube of the possible existence or non-existence of a wireless network associated with the target IP address. Further, the affiant failed to disclose whether or not the police had conducted an investigation to ascertain the existence or non-existence of such network.

51 Counsel agree that the correct approach to quash a search warrant is an application to a superior court of criminal jurisdiction for the extraordinary remedy of *certiorari*. Counsel further agree that the test to be applied by the reviewing superior court judge is set out in *R. v. Garofoli* (1990), 60 C.C.C. (3d) 161 (S.C.C.) at p. 188:

The reviewing judge does not substitute his or her view for that of the authorizing judge. If, based on the record which was before the authorizing judge as amplified on the review, the reviewing judge concludes that the authorizing judge could have granted the authorization, then he or she should not interfere. In this process, the existence of fraud, non-disclosure, misleading evidence and new evidence are all relevant, but, rather than being a prerequisite to review, their sole impact is to determine whether there continues to be any basis for the decision of the authorizing judge.

52 More recently in *R. v. Araujo*, 149 C.C.C. (3d) 449, 2000 SCC 65 (S.C.C.) at para. 54, LeBel J. crystallized the test as follows:

Again, the test is whether there was reliable *evidence* [as amplified] *that might reasonably be believed on the basis of which the authorization could have issued*, not whether in the opinion of the reviewing judge, the application should have been granted at all by the authorizing judge. [words in square bracket added].

53 Counsel for the applicant and the crown agreed to call evidence on the application. As mentioned, it was common ground that it is electronically possible for a neighbour to connect to the target IP address by means of a computer but only if the target IP address was an unsecured wireless network. There was no suggestion of fraud or misleading evidence.

54 Detective Barrie and Mr. Munster disagreed on the reliability of a signal strength of a wireless network to pinpoint the origin of a router in a residence. There was evidence on the application that the range of a wireless network might be affected by various factors, such as the location of the router in the residence.

2009 CarswellOnt 8689,

55 There was evidence that Mr. Brzezinski, Ms. Weiman and Jack Brzezinski lived at the target residence. Mr. Brzezinski was the account holder of the target IP address between January 6, 2009 and March 22, 2009 and the account was current. It is common ground that the target IP address was a candidate for downloading pornographic images, photographs and video. There was on the record, as amplified, reasonable grounds to believe that in the residence at 30 Gordon Rowe Crescent, Richmond Hill a computer system, device or media capable of storing computer data, photographs etc. would afford evidence of the commission of the offence. Similarly, there was reasonable grounds to believe that there is documentation at 30 Gordon Rowe Crescent that will assist in proving the identities of the residents who had control over the computer systems and stored data.

56 Detective Barrie testified that even if the pornographic data was not found on a computer or storage devices at 30 Gordon Crescent but there was a wireless network, a router may provide information concerning the identity of a computer which was a download candidate.

57 I conclude that the justice of the peace could have granted the search warrant based on the record before the authorizing judge as amplified by the evidence on the application before this Court.

FN1 See *R. v. Abadom* (1982), [1983] 1 All E.R. 364, [1983] 1 W.L.R. 126 (Eng. C.A.), lv. to app. ref'd. [1983] 1 W.L.R. 405 and *R. v. Terceira* (1998), 38 O.R. (3d) 175 (Ont. C.A.), at 183 -184, 189, affm'd. [1999] 3 S.C.R. 866 (S.C.C.) where statistics have been used by experts as part of their opinion.

END OF DOCUMENT

2012 CarswellOnt 12133, 2012 ONCA 660

2012 CarswellOnt 12133, 2012 ONCA 660

R. v. Ward

Her Majesty the Queen, Respondent and David Ward, Appellant

Ontario Court of Appeal

W. Winkler C.J.O., Doherty J.A., S.T. Goudge J.A.

Heard: January 12, 2012

Judgment: October 2, 2012

Docket: CA C50206

© Thomson Reuters Canada Limited or its Licensors (excluding individual court documents). All rights reserved.

Counsel: Jonathan Dawe, for Appellant

Michal Fairburn, for Respondent

James Stribopoulos, Lindsay Daviau, for Intervener, Canadian Civil Liberties Association

Subject: Constitutional; Criminal

Criminal law

***Doherty J.A.:***

**I**

1 Access to, the possession of, and trafficking in child pornography over the Internet present serious and pressing societal problems. Easy entry to the Internet, from almost anywhere, the international nature of the trade in child pornography, and user anonymity combine to make effective law enforcement difficult.

2 The police, in the course of investigating child pornography crimes on the Internet, sometimes request and receive the names and addresses of customers from Internet Service Providers ("ISP"). The police make this request following a protocol developed by the police and the ISPs, but without seeking or obtaining any prior judicial authorization. Using information gathered from other sources and the information provided by the ISP, the police can connect a customer's account to specific Internet activity. That connection may assist in developing reasonable and probable grounds to obtain a search warrant for the customer's residence and computer. Those searches may in turn lead to the discovery of child pornography, and the arrest and prosecution of the customer for child pornography offences.

2012 CarswellOnt 12133, 2012 ONCA 660

3 The police practice of seeking and obtaining customer information from ISPs and using that information to obtain search warrants has been constitutionally challenged as an unreasonable search and seizure in several cases. The majority of the cases have held that a customer does not have a reasonable expectation of privacy in the information provided by the ISP: *e.g.* see *R. v. Trapp*, 2011 SKCA 143, 377 Sask. R. 246, Ottenbreit J.A., concurring; *R. v. Spencer*, 2011 SKCA 144, 377 Sask. R. 280, Caldwell J.A., concurring; *R. v. Wilson*, [2009] O.J. No. 1067 (S.C.); *R. v. Vasic* (2009), 185 C.R.R. (2d) 286 (Ont. S.C.); *R. v. Brousseau*, 2010 ONSC 6753, 264 C.C.C. (3d) 562; and *R. v. McNeice*, 2010 BCSC 1544. Others have recognized a reasonable expectation of privacy in the information, but have held that the police acted reasonably in obtaining the information without prior judicial authorization: see *Trapp*, Cameron J.A., for the majority. Some cases have found a violation of s. 8 of the *Canadian Charter of Rights and Freedoms*: *e.g.* see *R. v. Kwok* (2008), 78 W.C.B. (2d) 21 (Ont. C.J.); *R. v. Cuttell*, 2009 ONCJ 471, 247 C.C.C. (3d) 424. This court addresses the constitutionality of this police practice for the first time. I would hold that in the circumstances presented here, the appellant has not established a reasonable expectation of privacy.

## II

### Overview and Position of the Parties

4 The police, in the course of a child pornography investigation, sought the name and address of a customer (sometimes referred to as subscriber information) from Bell Sympatico, a Canadian ISP. Bell Sympatico chose to cooperate with the police and provided what turned out to be the appellant's name and address. That information, combined with other information gathered by the police during their investigation, enabled the police to obtain a search warrant for the appellant's residence and his computer. That search yielded over 30,000 images of child pornography, along with about 373 videos containing child pornography. The appellant was charged with one count of possession of child pornography and one count of accessing child pornography.

5 At trial, the appellant defended the charges exclusively on the basis that the search of his residence and computer violated his rights under s. 8 of the *Charter*, and that s. 24(2) of the *Charter* required the exclusion of the evidence found in the search. The trial judge rejected the *Charter* claim and admitted the evidence: *R. v. Ward*, 2008 ONCJ 355, 176 C.R.R. (2d) 90. Convictions followed and the appellant was sentenced to 11 months' imprisonment and three years' probation. He appealed his convictions and sentences, but has abandoned his sentence appeal.

6 The appellant raises two grounds of appeal. Both repeat the arguments unsuccessfully advanced at trial. First, the appellant submits that he had a reasonable expectation of privacy in his subscriber information held by Bell Sympatico and that his constitutional right to be free from unreasonable search and seizure was violated when Bell Sympatico, at the request of the police, turned that information over to the police. The appellant contends that the police acted unconstitutionally in requesting and obtaining that information without prior judicial authorization, other lawful authority, the appellant's consent or exigent circumstances.

7 The appellant further submits that the information obtained through the unconstitutional seizure of his subscriber information was used to obtain the search warrant for his residence and computer and that without the subscriber information the police could not have obtained the warrant. It follows, the appellant argues, that if the subscriber information was obtained unconstitutionally, the search warrant is invalid, rendering the search of the appellant's residence and seizure of his computer unlawful and contrary to s. 8.

8 Finally, the appellant contends that the fruits of the search should have been excluded under s. 24(2). As it is common ground that without the seized evidence the Crown had no case, the appellant asks the court to quash the convictions and enter acquittals.

9 The appellant's second argument focuses on the adequacy of the contents of the information sworn to obtain the

2012 CarswellOnt 12133, 2012 ONCA 660

search warrant (ITO), and assumes that the police had lawfully obtained the appellant's subscriber information from Bell Sympatico. The appellant submits that the totality of the evidence relied on in the ITO did not provide grounds upon which a justice of the peace, acting judicially, could issue a search warrant. As with the first ground of appeal, the appellant contends that if this argument succeeds, the search and seizure violate s. 8, the evidence should be excluded under s. 24(2), and acquittals must follow.

10 The Crown responds that the trial judge correctly found that the appellant had no reasonable expectation of privacy in respect of his subscriber information held by Bell Sympatico. Absent a reasonable expectation of privacy, there could be no breach of the appellant's rights under s. 8 when the police acquired that information from Bell Sympatico. On the second issue, the Crown submits that on a review of the entirety of the ITO, there were ample grounds upon which the justice of the peace could, acting judicially, issue the warrant. Finally, the Crown argues that if either of the appellant's arguments succeeds, the fruits of the search of the appellant's residence and the seizure of his computer should not be excluded under s. 24(2) and the convictions should stand.

11 The grounds of appeal do not require any discussion of the factual merits of the allegations. The exclusion of the evidence under s. 24(2) of the *Charter* was the appellant's only hope for acquittals. If the evidence was admissible, the appellant's guilt was established beyond any reasonable doubt.

### III

#### Issue #1: Did The Appellant Have a Reasonable Expectation of Privacy in the Subscriber Information

##### A. The Trial Judge's Reasons

12 The trial judge correctly recognized that the appellant could not successfully advance a s. 8 claim unless he could demonstrate that he had a reasonable expectation of privacy in respect of the subscriber information held by Bell Sympatico. The trial judge, again correctly, understood that in determining whether the appellant had demonstrated a reasonable expectation of privacy, he had to consider the totality of the circumstances, including whether the appellant had a subjective expectation of privacy in respect of that information: see *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at paras. 18-19; *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579, at paras. 26-27; and *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211, at para. 18, Deschamps J., concurring, at paras. 77-78, Abella J., concurring.

13 The trial judge focussed his analyses on three factors. First, he noted that the requests for assistance made by the RCMP and Bell Sympatico's cooperation with those requests conformed to the federal legislation governing disclosure of customer information to law enforcement by private sector organizations such as Bell Sympatico.

14 Second, the trial judge referred, at some length, to the terms of the service agreement between the appellant and Bell Sympatico, and the documents related to that service agreement. That agreement addressed both Bell Sympatico's commitment to maintaining the confidentiality of client information, and its willingness to disclose client information to law enforcement authorities in connection with criminal investigations involving allegations of the criminal misuse of Bell Sympatico's services.

15 Lastly, the trial judge emphasized the nature of the information turned over to the RCMP by Bell Sympatico. In his view, that information, the appellant's name and address, was not the kind of information that would reveal intimate personal details or lifestyle choices. The trial judge concluded his analysis of the totality of the circumstances at para. 68 of his reasons:

[T]he name and address was in the hands of a third party. The third party was entitled to measure its obligation to maintain confidentiality over personal information in accordance with its contractual arrangement with the subscriber. Although the applicant had a subjective expectation of privacy, I find in looking at the totality of the



2012 CarswellOnt 12133, 2012 ONCA 660

evidence that there was no objective reasonable expectation of privacy. In other words the subjective expectation was not objectively reasonable having regard to all contextual factors and the totality of the circumstances.

16 The trial judge's finding that the appellant had no reasonable expectation of privacy in the subscriber information decided the s. 8 claim against the appellant. The trial judge had no need to go on and consider the reasonableness of the police conduct in obtaining the information from Bell Sympatico.

### ***B. The "Totality of the Circumstances" in This Case***

17 As the trial judge's reasons demonstrate, the totality of the circumstances engaged in this case has technical, investigative, legislative and contractual components. I will examine each separately. In doing so, I have tried to remain within the four corners of the trial record, although counsel, in an effort to educate the court (or at least one member of the panel), did refer to some aspects of the operation of the Internet, which they agreed were common knowledge.

18 I refer specifically to the need to stay within the evidentiary record, usually a self-evident proposition, because a review of other cases that have addressed this same issue suggests an understanding of the nature of an Internet protocol address ("IP address") that is different than that offered by the evidence in this case. Some cases indicate that the IP address is "unique to that subscriber", e.g., *Kwok*, at para. 8, and that armed with subscriber information and an IP address the police can compile a "history of [the subscriber's] activity on that network": *Trapp*, at para. 36, Cameron J.A., for the majority, at para. 78, Ottenbreit J.A., concurring. As outlined below, the evidence in this case does not support the contention that IP addresses are unique to individual subscribers or that combining an IP address with subscriber information allows the police to compile a history of a person's activity on the Internet. On this record, what is revealed is more in the nature of a snapshot than a history of one's Internet activity.

#### ***(i) The Technical Information***

19 The Internet, as a global system of computer networks, has become an increasingly important tool for the exchange of information. Internet use for a variety of reasons is ubiquitous in today's society. In many ways, the Internet has become the new library, shopping mall, theatre, meeting hall, and enumerable other venues all rolled into a single global venue available at the user's fingertips wherever he or she might be.

20 Generally speaking, access to the Internet is provided to individual subscribers through an ISP. A subscriber connects to the ISP network which in turn connects the subscriber to the Internet. The subscriber pays a fee for that service. There are a number of Canadian ISPs, including Bell Sympatico.

21 An IP address is a multi-digit numerical identifier that is automatically and randomly assigned by an ISP to a subscriber when the subscriber's computer device connects to the Internet. For example, one of the IP addresses identified on this appeal was 69.159.6.125. There are over 4.3 billion IP addresses worldwide. IP addresses are reused and are not unique to individual subscribers, although at any given point in time, an IP address will be assigned to a specific subscriber.

22 IP addresses belong to an ISP and are controlled by that ISP. The service agreement between Bell Sympatico and the appellant reflects the nature of an IP address in these terms:

Any IP address ... is the property of Your Service Provider at all times, and may be changed or withdrawn at any time in the sole discretion of Your Service Provider.

23 The ISP records the dates and times that its IP addresses are assigned to its subscribers. These records identify the subscribers' accounts on which the Internet was accessed at particular times. However that does not necessarily

2012 CarswellOnt 12133, 2012 ONCA 660

mean that the subscriber himself or herself was using the computer connected to the Internet at that time, or that it was even the subscriber's computer that was connected to the Internet. A wired or wireless network may link multiple computers to a central device referred to as a shared access point. When more than one computer is accessing the Internet through a shared access point at the same time there are additional technical issues that may arise. However, this case is not concerned with multiple computers sharing an access point.

24 IP addresses are usually assigned randomly and can be changed by the ISP at any time. An IP address is generally assigned by the ISP when a subscriber connects to the Internet. The same IP address may last for the duration of the Internet connection or it may change during the same connection. A subscriber will usually receive a new IP address each time he or she connects to the Internet. It is unlikely that a subscriber will be assigned the same IP address on two different connections to the Internet. However, subscribers who leave their computer or device connected to the Internet continually could use the Internet on separate occasions while retaining the same IP address.

25 The dynamic nature of an IP address is demonstrated in the details of the requests for information made in this case. The police asked Bell Sympatico for the name and address of the subscriber associated with an IP address used on June 16, 2006 between 06:09:24 and 06:09:48, a span of 24 seconds. The other two requests relating to connections made on July 2 and July 6 referred only to a single point in time. The information requested could not, in and of itself, reveal to the police anything about the subscriber's computer activity before or after the three connections referred to in the requests.

26 The IP address being used at any particular point in time to connect a computer or a wired or wireless network to specific content on the Internet can be determined in various ways. As happened in this case, some website operators record the IP addresses of users who access their site. Those operators might choose to share that information with the police. If the police have a specific IP address, they can, by accessing a website that is available to the public, identify the ISP that controls that IP address and a geographic location where it is being used. In this case, three IP addresses were identified as belonging to Bell Sympatico at Sudbury.

*(ii) The Investigation*

27 Carokee.com is a website that has operated out of Germany since 2001. It offers online forums open to the general public on a wide variety of topics, such as politics and sports. Individuals can create their own forum or page, or they may use an existing forum to post messages and exchange information. The website includes about 25,000 pages. Persons who access the website can do so anonymously, by utilizing anonymous e-mail addresses.

28 In July 2006, the owner of the website filed a criminal complaint with the German police alleging that some 28 pages on the website were being used to exchange child pornography files. German authorities investigated and found that there were child pornographic images on 17 of the pages on the website.

29 The German authorities, by reference to the IP addresses provided to them by the owner of the website, determined that some of the child pornographic material was being accessed through Canadian ISPs. In August or September 2006, the German authorities forwarded a list of 229 IP addresses and the times and dates associated with the accessing of the child pornography to the RCMP, along with copies of the related child pornography. By accessing a public website, the RCMP determined that three of the IP addresses belonged to Bell Sympatico and were connected to the Sudbury area. The three IP addresses and the relevant times and dates of the Internet connections were:

- IP address 69.159.6.125 between 06:09:24 and 06:09:48 on June 16, 2006;
- IP address 69.159.10.48 at 04:35:40 on July 2, 2006; and
- IP address 69.159.7.45 at 06:06:04 on July 6, 2006.

2012 CarswellOnt 12133, 2012 ONCA 660

30 Access to the carookee.com site required a person to provide an e-mail address. The three connections described above had been made using temporary e-mail addresses obtained anonymously.

31 On November 22, 2006, the RCMP sent letters of request to Bell Sympatico asking for the subscriber information of the subscriber assigned the three IP addresses at the times set out above. The request indicated that it was being sent "in accordance with s. 7(3)(c.1) of the *Personal Information Protection Electronic Documents Act*", S.C. 2000, c. 5 ("*PIPEDA*"). I will discuss that request in more detail below.

32 Bell Sympatico chose to comply with the requests. Bell Sympatico provided the name and address of the subscriber — the appellant, David Ward. It did not provide any other information.

33 After receiving the subscriber information, the RCMP contacted the Sudbury Police. Detective Constable Burt took carriage of the investigation for that force. He viewed the images that had been provided to the RCMP by the German authorities. The first incident, on June 16, 2006, involved the accessing of six images, each depicting a prepubescent boy with an erect penis. The second and third incidents, on July 2 and July 6, 2006, involved the downloading of an image of a prepubescent boy with an erect penis. The same image was downloaded on both dates. Detective Constable Burt was satisfied that all of the images accessed on the three dates fell within the legal definition of child pornography.

34 Detective Constable Burt and others on the Sudbury Police force conducted further investigations. Several sources confirmed that the appellant lived at the residence. Another officer was also able to confirm that the appellant lived alone, had a computer, did not employ a wireless network, and was a customer of Bell Sympatico. Armed with this information, the information provided by the German authorities, knowledge of the nature of the images, and the subscriber information provided by Bell Sympatico, the Sudbury Police applied for a search warrant.

35 On May 23, 2007, the Sudbury Police obtained a warrant to search the appellant's residence. They executed the warrant the next day, while the appellant was home alone. When the police entered the house, they saw child pornography on the appellant's computer screen. The police seized four computers and related material. Forensic analysis revealed over 30,000 images and 373 videos of child pornography.

(iii) *The Legislative Context: PIPEDA and the Criminal Code*

36 Several Canadian ISPs, including Bell Sympatico, have developed a protocol in conjunction with various Canadian law enforcement agencies to be used when those agencies are seeking subscriber information associated with the use of a specified IP address at a specific date and time. The protocol applies to child sexual exploitation investigations: see Suzanne Morin, "Updated: Business Disclosure of Personal Information to Law Enforcement Agencies: PIPEDA and the CNA Letter of Request Protocol", *Privacy Pages: CBA National and Privacy Access Law Section Newsletter* (November 2011), pp. 1-20.

37 Under the protocol, the police send a requesting letter to the ISP identifying the requesting officer, indicating that the officer is conducting an investigation in relation to child exploitation offences under the *Criminal Code*, and seeking disclosure of the last known customer name and address of an account holder associated with a specified IP address used at a specific date and time. The letter states that the request is made pursuant to s. 7(3)(c.1) of *PIPEDA*. The officer identifies his authority for the request by reference to the legislation governing the particular police force and the common law police powers. The letter provides no details of the specific investigation.

38 The requesting letter contains a space where the information sought by the police can be inserted by the ISP. If the ISP chooses to provide that information, it fills in the space and returns the letter to the requesting officer.



2012 CarswellOnt 12133, 2012 ONCA 660

39 In this case, Bell Sympatico received requests, referable to each of the three IP address connected to images of child pornography. These requests complied with the protocol. Bell Sympatico chose to cooperate with the requests, inserted the appellant's subscriber information in the letters and returned them to the RCMP.

40 *PIPEDA*, the statutory authority referred to in the form letter, is federal legislation governing the collection, use and disclosure of customers' personal information in the private sector. *PIPEDA* applies to any "organization" — a broadly defined term in the Act — that collects, uses or discloses the "personal information" — again a broadly defined term in the Act — in the course of their commercial activities: *PIPEDA*, ss. 2 and 4. *PIPEDA* applies to Bell Sympatico's disclosure of its customers' personal information.

41 *PIPEDA* recognizes and seeks to protect an individual's right to privacy in respect of personal information provided to organizations. At the same time, *PIPEDA* acknowledges that disclosure of that information by those organizations will in some circumstances be reasonable and appropriate. The dual rationale underlying the legislation is reflected in s. 3:

The purpose of this Part is to establish, in an era in which technology increasingly facilitates the circulation and exchange of information, rules to govern the collection, use and disclosure of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

42 Subsection 5(3) further confirms reasonableness as the touchstone of permissible disclosure of personal information under the Act:

An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.

43 Subsection 5(1) of *PIPEDA* requires that an organization, like Bell Sympatico, comply with the obligations set out in Schedule 1 of the Act. That schedule details the "Principles Set Out in the National Standard of Canada Entitled *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96". The principles found in Schedule 1 begin from the premise that an organization cannot disclose personal information obtained from a customer without the knowledge and consent of the customer. As s. 3 and s. 5(3) acknowledge, however, disclosure is appropriate in certain circumstances. Subsection 7(3) of the Act sets out circumstances in which an organization may, if it chooses to do so, disclose a customer's personal information without the customer's knowledge or consent. Some of the circumstances described in s. 7(3) contemplate disclosure to governmental authorities, including the police. For present purposes, the relevant disclosure provision is s. 7(3)(c.1)(ii):

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

...

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

...

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

2012 CarswellOnt 12133, 2012 ONCA 660

[Emphasis added.]

44 In this case, the letters of request sent by the RCMP to Bell Sympatico identified the "government institution" making the request — the RCMP; identified the "lawful authority" for the request — the *Royal Canadian Mounted Police Act*, the Royal Canadian Mounted Police Regulations, and the common law; and indicated that the disclosure was requested only for the purpose of an investigation in relation to child sexual exploitation offences under the *Criminal Code*, a "law of Canada".

45 The disclosure contemplated by s. 7(3) is discretionary. The organization asked to make disclosure of customer records must exercise that discretion in accordance with the overarching principle enunciated in s. 5(3) of *PIPEDA*. The disclosure must be for purposes that "a reasonable person would consider are appropriate in the circumstances." In exercising that discretion, the organization is entitled to consider factors such as the nature of the investigation, and the nature of the information requested: see Andrea Slane & Lisa M. Austin, "What's in a Name? Privacy and Citizenship in the Voluntary Disclosure of Subscriber Information in Online Child Exploitation Investigations" (2011) 57 *Crim. L.Q.* 486, at pp. 496-498.

46 The trial judge found, at para. 57 of his reasons, and the parties and the intervener agree, that *PIPEDA* does not create any police search and seizure powers. I agree with this interpretation. *PIPEDA* sets out the circumstances in which organizations may lawfully choose to disclose personal customer information, which must normally be kept confidential, to third parties including, in some circumstances, the police.

47 Crown counsel acknowledges that nothing in *PIPEDA* empowers the state to interfere with an individual's rights under s. 8 of the *Charter*. It does not follow that because an organization can disclose information to the state under *PIPEDA* that an individual has no privacy interest as against the state in that information for the purposes of s. 8. The terms of *PIPEDA* are, however, relevant to the s. 8 analysis to the extent that they speak to the existence and scope of a reasonable expectation of privacy in respect of information in the hands of an organization operating under the auspices of *PIPEDA*.

48 Subsection 487.014(1) of the *Criminal Code* is also germane given the disclosure regime established by *PIPEDA*:

For greater certainty, no production order is necessary for a peace officer ... enforcing or administering this or any other Act of Parliament to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing.

49 Subsection 487.014(1) seems to state the self-evident, perhaps explaining the opening phrase "for greater certainty". The section provides that where a person is not prohibited by law from disclosing information, the police may request disclosure of that information without prior judicial authorization. Read with *PIPEDA*, s. 487.014(1) allows the police, without obtaining prior judicial authorization, to ask an organization for information which that organization is lawfully entitled to disclose under *PIPEDA*.

50 With respect to the contrary opinion reached by the majority in *Trapp*, at para. 66, I do not read s. 487.014(1) as creating or extending any police search or seizure power. The police request identified in the section, standing alone, is not a search or seizure. The request, coupled with the voluntary cooperation with the request by the third party holder of the information, may or may not be a search or seizure depending on whether a claimant can establish a reasonable expectation of privacy in the information as against the state. That determination will depend on an assessment of the totality of the circumstances. Legislative provisions affecting either the police authority to request the information from third parties, e.g. s. 487.02(1), or the third party's ability to voluntarily disclose that information to the police, e.g. *PIPEDA*, are relevant to the reasonable expectation of privacy inquiry but do not create police powers to search or

2012 CarswellOnt 12133, 2012 ONCA 660

seize.

51 The appellant does not challenge the constitutionality of either *PIPEDA* or s. 487.014(1).

(iv) *The Service Agreement*

52 The relationship between Bell Sympatico and the appellant was governed by a service agreement and related documents setting out the terms on which Bell Sympatico agreed to provide services, including Internet connection, to the appellant. The contract between Bell Sympatico and the appellant is a classic contract of adhesion. Bell Sympatico unilaterally set the terms of the service agreement and related documents. If the appellant wanted the service provided by Bell Sympatico, he had to agree to Bell Sympatico's terms.

53 The terms of the service agreement included the following:

You will not use the Service in a manner that is contrary to any applicable law or regulation, and you will abide by Your Service Provider's policies, including without limitation the Acceptable Use Policy, which set forth additional rules that govern your activity in connection with the Service.

54 The Acceptable Use Policy ("AUP") attached to the service agreement provided that any violation of the AUP constituted a violation of the service agreement that could result in termination of the agreement. The AUP specifically prohibited:

5. Uploading or downloading, transmitting, posting, publishing, disseminating, receiving, retrieving, storing or otherwise reproducing, distributing or providing access to information, software, files or other material which ... (ii) are defamatory, obscene, child pornography or hate literature....

...

11. Transmitting, posting, receiving, retrieving, storing or otherwise reproducing, distributing or providing access to any program or information constituting or encouraging conduct that would constitute a criminal offence....

12. Violating or breaching any applicable law....

[Emphasis added.]

55 Paragraph 17 of the service agreement put the appellant on notice that Bell Sympatico reserved the right:

from time to time to monitor the Service electronically ... and to disclose any information necessary to satisfy any laws, regulations or other governmental request from any applicable jurisdiction, or as necessary to operate the Service or to protect itself or others.

[Emphasis added.]

56 In the AUP, Bell Sympatico made it clear that it would:

offer full co-operation with law enforcement agencies in connection with any investigation arising from a breach of this AUP.

2012 CarswellOnt 12133, 2012 ONCA 660

[Emphasis added.]

57 The service agreement also addressed the privacy features Bell Sympatico offered to its customers. In the agreement, Bell Sympatico undertook to protect its clients' "personal information" in a manner that was consistent with Bell Customer Privacy Policy and the Bell Code of Fair Information Practices. While it is not entirely clear, it would appear that the name and address of a customer, standing alone, would not qualify as "personal information" for the purposes of Bell's privacy policy and practices.

58 The service agreement further provided that customers like the appellant, by subscribing to the service, consented to the collection, use and disclosure of their personal information as described in Bell Sympatico's policies and practices, unless the customer specifically withdrew that consent by completing an "opt-out form". There is no evidence that the appellant "opted out".

### C. Legal Analysis

#### (i) A Broad and Purposive Interpretation of s. 8

59 Before examining the specific issues raised on this appeal, it is important to describe the jurisprudential landscape on which the issue raised by this ground of appeal must be resolved. I begin with the language of s. 8. It declares with eloquent simplicity that:

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

60 Section 8 stands as "a shield against unjustified state intrusions on personal privacy": *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456, at para. 8. Section 8 recognizes and constitutionally protects every person's right to live his or her life free of government intrusion except to the extent that the intrusion is reasonable. Personal privacy, broadly construed, includes control over one's body and bodily substances (physical privacy), control over certain places such as one's residence (territorial privacy), and control over information about the person and/or his activities (informational privacy): *Tessling*, at paras. 20-24.

61 The fundamental importance of personal privacy cannot be denied. Personal privacy is a prerequisite to individual liberty, security, self-fulfilment and autonomy. Personal privacy is also a precondition to the maintenance of a thriving democratic society: *R. v. Dymnt*, [1988] 2 S.C.R. 417, at pp. 427-428; *R. v. Wong*, [1990] 3 S.C.R. 36, at pp. 45-46; *R. v. Wise*, [1992] 1 S.C.R. 527, at p. 558, La Forest J., dissenting (but not on this point); *R. v. Plant*, [1993] 3 S.C.R. 281, at pp. 292-293; and *Tessling*, at paras. 12-16.

62 Section 8, like all *Charter* rights, must be interpreted broadly so as to best achieve the purpose underlying the right. As set out above, the protection of personal privacy from unreasonable state intrusion is the primary purpose of s. 8: *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, at pp. 158-159; *Dymnt*, at p. 253.

63 The purposive and broad interpretation of s. 8 is evident in the jurisprudence of the Supreme Court of Canada. Several facets of that jurisprudence are germane to this case. To begin with, the concepts of search and seizure are not defined by reference to the nature of the state conduct in issue, but primarily by reference to the effect of that conduct on the reasonable expectation of privacy of those targeted by the conduct: *R. v. Evans*, [1996] 1 S.C.R. 8, at para. 11; *R. v. Buhay*, 2003 SCC 30, [2003] 1 S.C.R. 631, at paras. 33-34; *R. v. Law*, 2002 SCC 10, [2002] 1 S.C.R. 227, at para. 15; *Wise*, at p. 538; *Tessling*, at para. 18; and *Gomboc*, at para. 77, Abella J., concurring.

64 Thus, while from the police perspective, it could be said that they merely asked Bell Sympatico for its assistance and Bell Sympatico volunteered its cooperation, from the appellant's perspective, the police, through their request and Bell Sympatico's cooperation, acquired personal information about the appellant's computer use that the



2012 CarswellOnt 12133, 2012 ONCA 660

appellant claimed he was reasonably entitled to expect would not be made available to the police without some prior judicial authorization. If the appellant had a reasonable expectation of privacy with respect to the information, the police acquisition of that information falls within the meaning of "search and seizure" for the purposes of s. 8 even though the state conduct was in no way coercive and Bell Sympatico voluntarily turned over the information.

65 A purposive reading of s. 8 also requires that the court identify the subject matter of the alleged search, not narrowly in terms of the physical acts involved or the physical space invaded, but rather by reference to the nature of the privacy interests potentially compromised by the state action. Thus, in *Patrick*, at para. 29, the court described the target of the search, not as the appellant's garbage bags left on the street, but rather as the appellant's personal information that could be gleaned from an examination of the contents of the garbage bags. In *Kang-Brown*, at para. 58, the court described the target of the search by the sniffer dog as the contents of the bag sniffed, and not merely the air surrounding the bag. Similarly, in *Tessling* and in *Gomboc*, the court characterized searches by reference to the information that could potentially be revealed about activities with the home and not simply as information about electricity or heat consumption within the home.

66 The proper characterization of the subject matter of the state conduct is important in this case. Ms. Fairburn, for the Crown, drawing on the analysis of the trial judge and that found in the concurring reasons of Ottenbreit J.A. in *Trapp*, at paras. 119-124 and 134, contends that the police acquired only the appellant's name and address, information that was readily available to the public and could not possibly be viewed as private or confidential by anyone. Ms. Fairburn further submits that the nature of the information obtained by the police from Bell Sympatico does not change because, when combined with information the police had obtained lawfully from other sources, it connects the appellant to certain Internet activity.

67 With respect to Ms. Fairburn's submissions, delivered with her customary clarity, her description of the target of the state action as the appellant's name and address is akin to the suggestion that the air around the bag was the target of the search conducted by the sniffer dog in *Kang-Brown*. That characterization does not describe what the police were really after, or what the appellant claims was within his reasonable expectation of privacy.

68 The police did not want the subscriber information so as to be able to identify the appellant as a customer of Bell Sympatico. That fact alone was of no value to the police. Nor does the appellant contend that he has a reasonable expectation of privacy with respect to the fact that he is a client of Bell Sympatico. The police wanted the information because they believed it could potentially identify the appellant as the person who had anonymously accessed child pornography on three separate occasions over the Internet. Translated into the content neutral language required for the purposes of s. 8, the police wanted the information because of what it could potentially tell them about the appellant's Internet activity on three occasions. They sought to connect an identity to certain activity: see *Slane & Austin*, at pp. 500-503.

69 I agree with Mr. Dawe, counsel for the appellant, that the reasonable expectation of privacy inquiry must be framed in terms of whether the police could access information "capable of revealing details about the appellant's Internet activities". I cannot, however, go so far as Mr. Dawe, and counsel for the intervener, who relying on the comments of Cameron J.A. in *Trapp*, at paras. 32-37, argue that the information sought by the police would provide "an electronic roadmap of the appellant's travels on the Internet". That description, while consistent with the language used in *Trapp*, at para. 36, goes beyond the evidentiary record in this case. Adapting the intervener's metaphor to the evidence adduced here, I would say that the police sought information capable of putting the appellant at a specific place, at a specific time in the course of his travels on the Internet.

70 The privacy claim advanced by the appellant raises a further important point about the scope of the privacy right protected by s. 8. The appellant is arguing that he had a reasonable expectation that he could access and use the Internet anonymously and that s. 8 protects him against state access to information in the hands of third parties that would allow the state to identify the appellant's activities on the Internet, unless the state can satisfy the reasonableness requirement of s. 8. The appellant in essence claims that his privacy rights under s. 8 protect his anonymity while

2012 CarswellOnt 12133, 2012 ONCA 660

engaged in certain activities, even activities in public venues.

71 Personal privacy is about more than secrecy and confidentiality. Privacy is about being left alone by the state and not being liable to be called to account for anything and everything one does, says or thinks. Personal privacy protects an individual's ability to function on a day-to-day basis within society while enjoying a degree of anonymity that is essential to the individual's personal growth and the flourishing of an open and democratic society.

72 In *Wise*, at p. 538, the court recognized an individual's expectation of privacy while engaged in very public activity. The court held that continual state electronic monitoring of the movements of an individual's vehicle on public highways violated that person's reasonable expectation of privacy. I take the court to have held that in Canadian society people can reasonably expect that they can move about on public highways without being identified and continually monitored by the state. If the state chooses to engage in that kind of invasive conduct, it must be able to meet the constitutional requirements of s. 8. *Wise* holds that while the public nature of the forum in which an activity occurs will affect the degree of privacy reasonably expected, the public nature of the forum does not eliminate all privacy claims.

73 The concept of privacy underlying *Wise* is described by Professor Westin as "public privacy": Alan F. Westin, *Privacy and Freedom* (New York: Athenum, 1967), at p. 32. He explains the relationship between anonymity and personal privacy in these terms, at p. 31:

The third state of privacy, anonymity, occurs when the individual is in public places or performing public acts but still seeks, and finds, freedom from identification and surveillance. He may be riding a subway, attending a ball game, or walking the streets; he is among people and knows that he is being observed; but unless he is a well-known celebrity, he does not expect to be personally identified and held to the full rules of behaviour and role that would operate if he were known to those observing him. In this state the individual is able to merge into the "situational landscape." Knowledge or fear that one is under systematic observation in public places destroys the sense of relaxation and freedom that men seek in open spaces and public arenas.

[Emphasis added.]

74 I think that s. 8 encompasses the concept of "public privacy" described above.[FN1] Surely, if the state could unilaterally, and without restraint, gather information to identify individuals engaged in public activities of interest to the state, individual freedom and with it meaningful participation in the democratic process would be curtailed. It is hardly surprising that constant unchecked state surveillance of those engaged in public activities is a feature of many dystopian novels.

75 By going on the website carookee.com, the appellant engaged with others in a public forum that was open to literally anyone around the world. The appellant did so, however, anonymously. Anonymity "to some degree at least" is a feature of much Internet activity: *Warman v. Wilkins-Fournier*, 2010 ONSC 2126, 100 O.R. (3d) 648, at para. 20 (Div. Ct.). Depending on the totality of the circumstances, his anonymity may enjoy constitutional protection under s. 8.

76 A purposive approach to s. 8 also dictates that personal privacy claims be measured as against the specific state conduct and the purpose for that conduct. Section 8 is not about protecting individual privacy at large or as between non-state actors. Section 8 focuses on personal privacy claims in relation to state intrusions said to infringe on that personal privacy: *Gomboc*, at para. 34, Deschamps J., concurring. Because the focus is on state intrusion and the purpose of the intrusion, Canadian jurisprudence has emphatically rejected the "risk" analysis featured in American Fourth Amendment jurisprudence: e.g. see *R. v. Duarte*, [1990] 1 S.C.R. 30, at p. 48; *Wong*, at p. 45. According to that jurisprudence, voluntary disclosure to third parties defeats Fourth Amendment claims: e.g. see *Smith v. Maryland*, 442 U.S. 735(1979), at pp. 743-744; *United States v. Miller*, 425 U.S. 435(1976), at pp. 442-443; and Robert W. Hubbard,

2012 CarswellOnt 12133, 2012 ONCA 660

Peter DeFreitas & Susan Magotiaux, "The Internet — Expectations of Privacy in a New Context" (2001) 45 Crim. L.Q. 170, at pp. 177-185.[FN2]

77 Under the Canadian jurisprudence, a person, by allowing others into a zone of personal privacy, does not forfeit a claim that the state is excluded from that same zone of privacy. Nor does allowing a state actor within a zone of personal privacy for a specified purpose, automatically foreclose a claim of privacy as against the state should it enter that same zone of privacy for another purpose: *R. v. Colarusso*, [1994] 1 S.C.R. 20, at p. 55; *Law*, at paras. 19-22; *Thomson Newspapers Ltd. v. Canada*, [1990] 1 S.C.R. 425; *Gomboc*, at paras. 100-102, McLachlin C.J.C. and Fish J., dissenting (but not on this point); *R. v. D'Amour* (2002), 166 C.C.C. (3d) 477 (Ont. C.A.), at para. 57; and *R. v. Cole*, 2011 ONCA 218, 105 O.R. (3d) 253, at paras. 74-78. On the purposive interpretation of s. 8, it is no answer to the appellant's s. 8 claim to assert that because the appellant willingly surrendered the relevant information to Bell Sympatico, he assumed the risk that Bell Sympatico would share the information with the police.

78 In holding that the risk that Bell Sympatico would share the information does not necessarily defeat a s. 8 claim, I do not suggest that the relationship between the appellant and Bell Sympatico, particularly as it related to any agreement concerning the disclosure of information, was not relevant to the appellant's privacy claim. I mean only to say that willing disclosure to third parties is not determinative of the existence of a legitimate privacy claim under s. 8.

(ii) *Section 8 Protects Only Reasonable Expectations of Privacy*

79 Despite the centrality of personal privacy to the relationship between the individual and the state under the Canadian constitution, personal privacy, like any other individual right, cannot be absolute in a democratic society. One's right to be left alone by the state must be balanced against other legitimate competing societal interests, including the need to effectively investigate crime: *Hunter*, at pp. 159-160; *Tessling*, at paras. 17-18. In *Hunter*, Dickson J. described the balance in these terms:

The guarantee of security from unreasonable search and seizure only protects a reasonable expectation. This limitation on the right guaranteed by s. 8, whether it is expressed negatively as a freedom from "unreasonable" search and seizure, or positively as an entitlement to a "reasonable" expectation of privacy, indicates 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.

[Emphasis added.]

80 The s. 8 jurisprudence strikes the balance between individual privacy and competing state interests by constitutionally protecting only privacy claims that are founded on a *reasonable expectation of privacy* and by prohibiting only state intrusions upon reasonable expectations of privacy that are *unreasonable*: *Tessling*, at paras. 17-18.

81 How then is one to determine whether a claimant has "a reasonable expectation of privacy"? In *Tessling*, at para. 42, Binnie J. observes that "[e]xpectation of privacy is a normative rather than a descriptive standard."

82 By "normative", I understand Binnie J. to mean that in determining whether an individual enjoys a reasonable expectation of privacy, the court is making a value judgment more than a finding of fact in the traditional sense. When the court accepts the contention that a person has a reasonable expectation of privacy, the court is in reality declaring that the impugned state conduct has reached the point at which the values underlying contemporary Canadian society dictate that the state must respect the personal privacy of individuals unless it is able to constitutionally justify any interference with that personal privacy.

83 The normative nature of the reasonable expectation of privacy inquiry has been underscored in several pro-

2012 CarswellOnt 12133, 2012 ONCA 660

nouncements from the Supreme Court of Canada beginning in *Wong*, at pp. 45-46, where La Forest J. described the inquiry in these terms:

[W]hether, by the standards of privacy that persons can expect to enjoy in a free and democratic society, the agents of the state were bound to conform to the requirements of the *Charter* when effecting the intrusion in question.

84 In *Patrick*, at para. 14, Binnie J. stressed the long-term consequences on personal privacy of the impugned state action in assessing the privacy claim:

Privacy analysis is laden with value judgments which are made from the independent perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy.

85 Most recently in *Gomboc*, Deschamps J., at para. 34, in her concurring reasons, captured the normative nature of the inquiry in these terms:

Thus, the fact that the person claiming an expectation of privacy in information ought to have known that the terms governing the relationship with the holder of that information allowed disclosure may not be determinative. Rather, the appropriate question is whether the information is the sort that society accepts should remain out of the state's hands because of what it reveals about the person involved, the reason why it was collected, and the circumstances in which it was intended to be used.

[Emphasis added.]

86 The courts have approached the reasonable expectation of privacy inquiry by asking whether the claimant had a subjective expectation of privacy and, if so, whether in all of the circumstances that expectation was reasonable: e.g. see *R. v. Edwards*, [1996] 1 S.C.R. 128, at para. 45; *R. v. Nolet*, 2010 SCC 24, [2010] 1 S.C.R. 851, at para. 30. While both questions help to focus the inquiry on the specific facts of the case and the values underlying s. 8, neither question captures the entirety of the reasonable expectation of privacy inquiry. Section 8 is concerned with the degree of privacy needed to maintain a free and open society, not necessarily the degree of privacy expected by the individual or respected by the state in a given situation. As Binnie J. put it in *R. v. A.M.*, 2008 SCC 19, [2008] 1 S.C.R. 569 at para. 33, s. 8 protects the privacy interests that:

the citizen subjectively believes ought to be respected by the government and "that society is prepared to recognize as 'reasonable'"....

[Emphasis added; citation omitted.]

87 The fact that the paranoid target of a search has no expectation of privacy cannot negative his s. 8 rights: see *Tessling*, at para. 42. Nor can ubiquitous state intrusions upon privacy render expectations of privacy unreasonable for the purposes of s. 8: see *Patrick*, at para. 14. The ultimate question is whether the personal privacy claim advanced in a particular case must, upon a review of the totality of the circumstances, be recognized as beyond state intrusion absent constitutional justification if Canadian society is to remain a free, democratic and open society: see James A. Q. Stringham, "Reasonable Expectations Reconsidered: A Return to the Search for a Normative Core of Section 8?" (2005) 23 C.R. (6th) 245.

88 As has repeatedly been said, the reasonable expectation of privacy inquiry is contextual and looks at the totality of the circumstances: *Edwards*, at paras. 31-45; *Tessling*, at paras. 19 & 31; and *Patrick*, at para. 26. Importantly, this contextual examination has no regard to the product of the challenged search or seizure. The inquiry is framed in



2012 CarswellOnt 12133, 2012 ONCA 660

"broad and neutral terms": *Wong*, at p. 50; see also *Buhay*, at para. 19; *Patrick*, at para. 32. The question is not whether the appellant had a reasonable expectation that he could access and possess child pornography anonymously. The question is whether the appellant had a reasonable expectation that he could anonymously access the Internet on his computer without the state, with the cooperation of the appellant's ISP, being able to find out what he had accessed.

(iii) *The Application of the Principles to this Case*

89 The appellant presents his privacy claim as informational in nature. He asserts a right to privacy as against the state in certain information held by a third party, Bell Sympatico. The appellant maintains that the right to privacy over that information arises because if the information is disclosed to the state, the state will be able to identify some of the appellant's Internet activity and thereby obtain personal information that could reveal intimate details about the appellant's lifestyle and personal choices: see *Plant*, at p. 293. Given that the information provided to the police by Bell Sympatico ultimately revealed the appellant as the person who accessed child pornography on three occasions, it is difficult to argue with the contention that the information provided by Bell Sympatico had the potential to open doors into very private aspects of the appellant's lifestyle.

90 I agree with the parties that the issue is properly framed in terms of a claim to privacy in information. In so holding, I do not ignore the fact that the activity was carried out in the appellant's residence thereby potentially raising a territorial privacy claim of the highest order. However, the physical location where the Internet activity occurred seems entirely incidental to the activity itself. The appellant's privacy claim comes down to an assertion of a reasonable expectation of anonymity when on the Internet. The anonymity claim is tied to the nature of the activity, not to the location where the activity occurs. For that reason, this case is distinguishable from cases like *Tessling* and *Gomboc* in which the activities potentially revealed to the police had a strong physical connection to the claimant's residence.

91 Not only is the appellant's privacy claim advanced in relation to information, that information was obtained from a third party, Bell Sympatico, who had acquired it from the appellant in the course of a commercial relationship. The Supreme Court of Canada has addressed this kind of privacy claim in *Plant*, *Tessling* and *Gomboc*. Those cases identify a number of factors relevant to the reasonable expectation of privacy inquiry. I propose to examine the factors that are important in the circumstances of this case by addressing three questions:

- What was the subject matter of the impugned state conduct, that is, what were the police after when they asked Bell Sympatico for the subscriber information?
- Did the appellant have a subjective expectation that he could act with anonymity, at least with regard to the state, in his Internet activity?
- If so, was that expectation objectively reasonable?

**(a) The Target of the Police Action**

92 As discussed earlier, the police were after information that would potentially identify the appellant, not merely as a Bell Sympatico subscriber, but a person who had engaged in certain activities on three specific occasions on the Internet. The information sought by the police would strip the appellant of his Internet anonymity on those three occasions. This characterization of the target of the police action is not in any way altered because the information provided by Bell Sympatico would not conclusively identify the appellant as the person engaged in those activities. The information would connect his account to those activities and go some distance to identifying him as the person involved in those activities.

93 Information that has the very real potential to reveal activities of a personal and private nature is, in my

2012 CarswellOnt 12133, 2012 ONCA 660

opinion, "information which tends to reveal intimate details of the lifestyle and personal choices of the individual": *Plant*, at p. 293. It follows that information that has the potential to reveal activities of that kind may be deserving of constitutional protection. The nature of the information does not, however, mean that it automatically attracts constitutional protection under s. 8. The totality of the circumstances must be considered. Where the information has been given by the claimant to a third party who in turn provides it to the police, the relationship between the claimant and that third party as it relates to the information is of critical importance. I will turn to that relationship after addressing the appellant's subjective expectation of privacy.

### **(b) The Subjective Expectation of Privacy**

94 The trial judge found that the appellant had a subjective expectation of privacy in respect of his subscriber information. When, as in my view it should be, the information is characterized as information revealing the appellant's Internet activity, there can be no doubt that he had a subjective expectation of privacy. The appellant did not reveal his identity when accessing the sites and used temporary anonymous email addresses suggesting a clear intention to conceal his identity even further. The Crown's submission that the appellant was not "fussed about keeping his name and address private" misses the distinction between identifying the appellant as a Bell Sympatico subscriber and identifying the appellant's Internet activity. I think the appellant was clearly "fussed" about keeping his identity private as it related to his Internet activities.

### **(c) Is the Expectation Objectively Reasonable: The Relationship Between the Appellant and Bell Sympatico**

95 The appellant and Bell Sympatico had a commercial relationship whereby Bell Sympatico provided a variety of services, including Internet access to the appellant for a fee. Unlike for example a doctor-patient relationship, there was nothing inherently confidential in the relationship between Bell Sympatico and the appellant. In the private law context, their relationship, including any obligation Bell Sympatico had to maintain the confidentiality of information provided by the appellant, was governed by the terms of the service agreement between Bell Sympatico and the appellant, related documents referred to in the service agreement, and the terms of *PIPEDA*. As *Gomboc* demonstrates, it is necessary to look at the controlling contractual and legislative provisions when determining whether a person has a reasonable expectation of privacy in information that a third party service provider has given to the police.

96 To properly describe the relationship between the appellant and Bell Sympatico, one must first properly characterize Bell Sympatico's relationship with the police insofar as the request for the appellant's subscriber information is concerned. On this record, Bell Sympatico was not an agent of the police. Bell Sympatico had information in its possession over which it clearly had an interest. Bell Sympatico was not compelled by any statute to provide the information to the police. It chose to do so when faced with a very specific and narrow request and when made aware of the nature of the investigation: see *Gomboc*, at para. 42, Deschamps J., concurring[FN3] ; see also *McNeice*, at paras. 41-45.

97 Like any service provider, Bell Sympatico had a legitimate interest in preventing the criminal misuse of its services, particularly in circumstances where the misuse effectively constituted the *actus reus* of a crime. That interest may be seen as purely a self-interest or, perhaps more appropriately, as a form of "civic engagement" reflecting a corporate commitment to assist in law enforcement's struggle to rid the Internet of child pornography: see *Gomboc*, at paras. 41-42, Deschamps J., concurring; Slane & Austin, at p. 490.

98 The normative nature of the reasonable expectation of privacy analysis and the value judgments that underlie that analysis require that Bell Sympatico's legitimate interests, whether described as self-interest, civic engagement, or both, be taken into account in determining whether the appellant had a reasonable expectation of privacy in respect of the information held by Bell Sympatico. A reasonable and informed person considering whether society would find it reasonable for the appellant to have a reasonable expectation of privacy in his subscriber information would take into account Bell Sympatico's legitimate interests in voluntarily disclosing that information to the police when that dis-

2012 CarswellOnt 12133, 2012 ONCA 660

closure would assist in an investigation of the alleged criminal misuse of Bell Sympatico's services, assuming the disclosure was not prohibited and would not violate any laws or the terms of applicable customer agreement.

99 Bell Sympatico's legitimate interest in disclosing customer information to the police finds expression in the terms of *PIPEDA*. Those terms contemplate "reasonable disclosure" of customers' personal information and recognize a discretion to disclose personal information to the police in the course of an investigation if the prerequisites of the disclosure provision are met: *PIPEDA*, ss. 3, 5(3) and 7(3)(c.1)(ii).

100 Setting aside the contractual terms for the moment, I think the "reasonable and informed person" identified by Binnie J. in *Patrick*, at para. 14, would view a customer's reasonable expectation of privacy in his or her subscriber information to be circumscribed by the service provider's discretion to disclose that information to the police where it was both reasonable to do so and a *PIPEDA* compliant request for disclosure had been made by the police.

101 The requests made in this case complied with s. 7(3)(c.1)(ii) of *PIPEDA*. In considering whether Bell Sympatico acted reasonably in disclosing the information, the nature of the information sought is relevant. The police request was specific and narrow. They sought only the client's name and address. That information in and of itself revealed nothing personal about the appellant or his Internet usage. The request was also narrow in the sense that it identified three specific instances of Internet activity. By disclosing the subscriber information to the police, Bell Sympatico would not be telling the police anything about the client's Internet activities at any time other than three times identified in the requests.

102 I think it is also significant that the request referred specifically to the investigation of child exploitation offences under the *Criminal Code*. Bell Sympatico was entitled to have regard to the nature of the offences being investigated when it decided whether to disclose the information. These offences are obviously serious. They victimize children, a very vulnerable element of the community and one which the community, as a whole, has a responsibility to protect. Further, Bell Sympatico's service was an integral and essential component of the offences being investigated. In a very real sense, the power and anonymity of the Internet allows these kinds of offences to be committed. The alleged perpetrator had gained access to this powerful and anonymous tool through the services provided by Bell Sympatico. The strong and direct connection between Bell Sympatico's services and the commission of the crimes under investigation would, in my view, make it all the more reasonable to expect that Bell Sympatico would cooperate with the police request for subscriber information.

103 In stressing the nature of the offence under investigation, I do not fall into the trap of judging the appellant's privacy expectation by reference to the nature of his activity. The nature of the offence under investigation is relevant to the reasonableness of Bell Sympatico's response to the police request. The nature of the activity that would actually be revealed to the police by the information provided by Bell Sympatico is not germane to the reasonable expectation of privacy inquiry.

104 I see some analogy between my reliance on *PIPEDA* and the reliance of Abella J. in her concurring reasons in *Gomboc* on the terms of a regulation that allowed the utility supplier to provide information to the police absent an express request for confidentiality by the client. As Abella J. did in *Gomboc*, I look to legislation, the constitutionality of which is not challenged, and which by its terms speaks to the circumstances in which the third party holder of the information may disclose that information to the police as informing the degree of privacy that persons ought reasonably to expect in our society.

105 My analysis of the impact of *PIPEDA* on the reasonable expectation of privacy inquiry is somewhat at odds with that of Cameron J.A. who considered the provincial equivalent to *PIPEDA* in *Trapp*, at paras. 49-54. I agree with Cameron J.A. that the reasonable expectation of privacy inquiry must proceed on the basis that the service provider will exercise "a meaningful measure of independent and informed judgment" in deciding whether to make the disclosure requested by the police: at para. 55. However, I am satisfied that having regard to the nature of the disclosure

2012 CarswellOnt 12133, 2012 ONCA 660

requested in this case, and the nature of the crimes being investigated, that the reasonable informed person would accept that it was reasonable for the ISP to make the disclosure requested. If disclosure by the ISP was a reasonable response to the request then, in these circumstances, the appellant's privacy claim in the face of the request is not objectively reasonable.

106 I come finally to the contractual terms. Unlike the provision in *Gomboc*, there is no legislative authority underlying the terms of the service agreement between Bell Sympatico and the appellant. Also, the caution sounded by Deschamps J. in *Gomboc*, at para. 33, against reliance on the terms of contracts of adhesion when deciding constitutional rights has application here.

107 The contractual provisions in this case tend to reinforce my reliance on *PIPEDA* as indicative of the nature of the appellant's reasonable expectation of privacy. Like *PIPEDA*, the contractual terms speak both of Bell Sympatico's duty to protect the privacy of clients' information and its willingness to disclose information in relation to investigations involving the alleged criminal misuse of its services. That willingness clearly qualifies any duty of confidentiality assumed by Bell Sympatico. While there is no single provision in the agreement or related documents that spells out Bell Sympatico's willingness to disclose information to the police as clearly as did the regulation under consideration in *Gomboc*, the overall thrust of the documentation is to the same effect. In particular, the Accepted Use Policy ("AUP") makes it clear that uploading or downloading child pornography is a breach of the AUP and that Bell Sympatico would "offer full cooperation with law enforcement agencies in connection with any investigation arising from a breach of this AUP." That cooperation would, it seems to me, obviously extend to the disclosure of subscriber information which, by the terms of the service agreement, could be disclosed if "[n]ecessary to satisfy any laws, regulations or other governmental request ... or as necessary ... to protect ... others."

108 My review of the terms of the service agreement and related documents reinforces my view that a reasonable and informed person would not expect that society should recognize that the appellant had a reasonable expectation of privacy in respect of the subscriber information held by Bell Sympatico.

109 I stress that the conclusion in this case is based on the specific circumstances revealed by this record and is not intended to suggest that disclosure of customer information by an ISP can never infringe the customer's reasonable expectation of privacy. If, for example, the ISP disclosed more detailed information, or made the disclosure in relation to an investigation of an offence in which the service was not directly implicated, the reasonable expectation of privacy analysis might yield a different result. Similarly, if there was evidence that the police, armed with the subscriber's name and address, could actually form a detailed picture of the subscriber's Internet usage, a court might well find that the subscriber had a reasonable expectation of privacy. Those cases will be considered using the totality of the circumstances analysis when and if they arise.

## Issue #2: The Adequacy of the ITO

110 The appellant's second ground of appeal challenges the information to obtain the search warrant (ITO) that authorized the search of the appellant's residence and computer. Counsel argues that even if all of the material contained in the ITO was properly included in that document, it did not provide sufficient grounds upon which the warrant could be issued. Counsel places heavy reliance on *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253. In *Morelli*, the court found that a warrant authorizing the search of an individual's computer for child pornography ought not to have been issued as it did not provide grounds upon which a justice of the peace could reasonably believe that the named person possessed child pornography on his computer.

111 The appellant made a similar argument at trial but did not have the benefit of *Morelli*. The trial judge found that the ITO contained sufficient grounds upon which the justice of the peace acting judicially could issue the warrant. He concluded that many of the appellant's arguments demonstrated only that the grounds in the ITO did not establish that the appellant had committed the offences referred to in the ITO. The trial judge correctly pointed out that the ITO



2012 CarswellOnt 12133, 2012 ONCA 660

need only provide reasonable grounds to believe that evidence relating to the offences would be found in the searches. The appellant's ultimate culpability was irrelevant to whether the warrant should issue.

112 The standard of review applicable to this argument is well settled. The trial judge was obliged to determine whether there were grounds upon which the issuing justice could grant the warrant. This court applies the same deferential standard: *R. v. Garafoli*, [1990] 2 S.C.R. 1421, at p. 1452. *Morelli* is an example of the application of the well-established *Garafoli* standard of review to the particular facts of that case. *Morelli* breaks no new jurisprudential ground.

113 This ITO is very different from the ITO found to be deficient in *Morelli*. Most significantly, this ITO provided strong evidence from which it could be inferred that someone using the appellant's computer at his residence had accessed or downloaded child pornography on eight instances, six on June 16, 2006 and one each on July 2 and 6, 2006. These allegations, in my view, provided a basis upon which the justice could infer that there was a reasonable probability that child pornography had been accessed and stored on the computer. Unlike *Morelli*, the police in this case sought the warrant both in respect of the offence of accessing child pornography and the offence of possessing child pornography. In *Morelli*, the police sought a warrant only in respect of the possession charge.

114 The ITO also provided extensive technical evidence to the effect that files downloaded by the appellant on the computer could be recovered by police technicians even if the appellant had made efforts to delete those files. This evidence offered some basis for an inference that the prohibited material remained on the computer long after it was downloaded and could be recovered if the police were given access to the computer.

115 The affiant also provided detailed evidence based on his first-hand experiences about the practices of individuals who access and possess child pornography on their computers. He indicated that often these individuals kept images for "long periods of time" and "rarely deleted collections". I see no reason why this kind of evidence, rooted in the officer's personal experience, could not provide some assistance in determining whether the warrant should be granted. I bear in mind that the officer's opinion did not stand alone. There was other reliable evidence that this computer had been used to access child pornography on three occasions over a three-week period suggesting use of the computer by someone with an interest in child pornography.

116 The technical evidence and the officer's opinion evidence provided a basis upon which a justice of the peace could reasonably infer that there was a reasonable probability that the child pornography that had been accessed on the computer some ten months earlier was still on the computer and could be retrieved by the police. That is all that was needed to justify the issuance of the warrant. This ground of appeal fails.

#### IV

#### Conclusion

117 I would dismiss the appeal.

***W. Winkler C.J.O.:***

I agree

***S.T. Goudge J.A.:***

I agree

2012 CarswellOnt 12133, 2012 ONCA 660

FN1 In *Tessling*, at para. 40, Binnie J. states "a person can have no reasonable expectation of privacy in what he or she knowingly exposes to the public". In my view, this comment is not directed at cases where the person acts anonymously: see also *Wise*, at p. 558, La Forest J., dissenting.

FN2 The "risk analysis" favoured in the American case law would doom the appellant's argument since the subscriber information was willingly disclosed to the appellant's ISP: e.g. see *United States v. Perrine*, 518 F. 3d 1196 (10th Cir. 1998), at pp. 1204-1205; *United States v. Bynum*, 604 F. 3d 161 (4th Cir. 2010), at p. 164. Recently, in *United States v. Jones*, 565 U.S. \_\_\_\_\_ (2012), Sotomayor J., in a concurring opinion, suggested that the risk analysis approach was "ill suited to the digital age in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks." She opined that it may be time to reconsider the court's approach to privacy claims under the Fourth Amendment.

FN3 The dissent in *Gomboc* views the utility company as having been conscripted to assist the police. This conclusion seems to be based on the utility company's installation, at the request of the police, of a special device used to generate, record and disclose the relevant information. Here, Bell Sympatico did nothing other than provide information from its database.

END OF DOCUMENT

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

R. v. Trapp

Brian Arnold Trapp (Appellant) and Her Majesty the Queen (Respondent)

Saskatchewan Court of Appeal

Cameron, Jackson, Ottenbreit JJ.A.

Heard: November 9, 2010

Judgment: November 25, 2011

Docket: 1802-CR

© Thomson Reuters Canada Limited or its Licensors (excluding individual court documents). All rights reserved.

Proceedings: affirming *R. v. Trapp* (2009), 344 Sask. R. 300, 2009 SKPC 109, 2009 CarswellSask 725 (Sask. Prov. Ct.)

Counsel: Ronald Piché, for Appellant

Graeme Mitchell, Q.C., for Crown

Subject: Criminal; Constitutional

Criminal law --- Offences — Obscenity and pornography — Child pornography — Elements

Accused's computer was connected to file-sharing network — Shared folder therein contained files with child pornography — Images showed inter alia children engaged in explicit sexual activity — Files were downloaded to accused's computer — Accused also had disk with story advocating sexual activity with person under 18 — Accused was charged with making available, accessing, and having in his possession child pornography — Accused convicted — Crown proved constituent elements of each offence — Accused appealed — Appeal dismissed — Accused enjoyed reasonable expectation of privacy in expectation of privacy in relation to subject matter of alleged breach and police intruded upon his privacy when it sought and obtained information in question from communication provider — Search occurred within meaning of s. 8 of Canadian Charter of Rights and Freedoms — Police had reasonable and probable grounds to believe that offence or offences against s. 163 of Criminal Code had been committed and that communication provider was in possession of information affording evidence thereof — Police had every reason to believe that the communication provider was not prohibited by law from disclosing information — Search was authorized by law, and manner in which search was conducted was reasonable.

The accused's computer was connected to a file-sharing network. The shared folder therein contained files with child pornography. The files were downloaded to the accused's computer. The police sought and obtained from a communication provider information regarding the Internet Protocol Address it had assigned to the accused in relation to his access to the Internet. The accused was convicted of making available, accessing, and having in his possession child pornography. The accused appealed.

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

**Held:** The appeal was dismissed.

Per Cameron J.A. (Jackson J.A. concurring): The question was whether the accused made out a sufficient case to engage s. 8 of the Canadian Charter of Rights and Freedoms. There was an objectively reasonable expectation of privacy in relation to the information and, hence, the subject matter of the alleged search. The accused enjoyed a reasonable expectation of privacy in relation to the subject matter of the alleged search and the police intruded upon his privacy when it sought and obtained the information in question from the communication provider. A search occurred within the meaning of s. 8 of the Charter. The police had reasonable and probable grounds to believe that an offence or offences against s. 163 of the Criminal Code had been committed and that the communication provider was in possession of information affording evidence thereof. The police had every reason to believe that the communication provider was not prohibited by law from disclosing this information. The search was authorized by law, and the manner in which the search was conducted was reasonable.

Per Ottenbreit J.A. (concurring): While it may be that a search and seizure of one's personal computer in one's home is an intrusive and extensive invasion of one's privacy, in this case the information received by the police by itself gave no access to the contents of the accused's computer. The search occurred at the offices of the communication provider, which was a place where the accused had no reasonable expectation of privacy whatsoever. The letter requesting information was not intrusive. It involved no interference with the accused's personal or bodily integrity. It involved no direct access to the house where the internet connection was located and by itself provided no particulars of what was going on in the house or the content of the use of the computer at the relevant time. The intrusion into privacy under these circumstances was a minimal and proportional way of determining who the anonymous user of the specific IP address was. In the circumstances, the information was collected for a legitimate purpose, the furtherance of the child pornography investigation. On the totality of circumstances, there was no reasonable expectation of privacy in the accused's name, address and phone number respecting his IP address. The trial judge made no error in finding there was no search and seizure and violation of s. 8 of the Charter.

**Cases considered by *Cameron J.A.*:**

*Canada (Director of Investigation & Research, Combines Investigation Branch) v. Southam Inc.* (1984), (sub nom. *Hunter v. Southam Inc.*) 11 D.L.R. (4th) 641, 33 Alta. L.R. (2d) 193, (sub nom. *Hunter v. Southam Inc.*) 55 A.R. 291, 27 B.L.R. 297, 41 C.R. (3d) 97, 84 D.T.C. 6467, (sub nom. *Hunter v. Southam Inc.*) 14 C.C.C. (3d) 97, (sub nom. *Director of Investigations & Research Combines Investigation Branch v. Southam Inc.*) [1984] 6 W.W.R. 577, 1984 CarswellAlta 121, 1984 CarswellAlta 415, (sub nom. *Hunter v. Southam Inc.*) [1984] 2 S.C.R. 145, (sub nom. *Hunter v. Southam Inc.*) 55 N.R. 241, (sub nom. *Hunter v. Southam Inc.*) 2 C.P.R. (3d) 1, (sub nom. *Hunter v. Southam Inc.*) 9 C.R.R. 355, 48 N.R. 320 (S.C.C.) — referred to

*R. v. Collins* (1987), [1987] 3 W.W.R. 699, [1987] 1 S.C.R. 265, (sub nom. *Collins v. R.*) 38 D.L.R. (4th) 508, 74 N.R. 276, 13 B.C.L.R. (2d) 1, 33 C.C.C. (3d) 1, 56 C.R. (3d) 193, 28 C.R.R. 122, 1987 CarswellBC 94, 1987 CarswellBC 699 (S.C.C.) — followed

*R. v. Cuttell* (2009), 203 C.R.R. (2d) 342, 247 C.C.C. (3d) 424, 2009 CarswellOnt 5896, 2009 ONCJ 471 (Ont. C.J.) — referred to

*R. v. Gomboc* (2010), 328 D.L.R. (4th) 71, [2010] 3 S.C.R. 211, 263 C.C.C. (3d) 383, 79 C.R. (6th) 199, 408 N.R. 1, 34 Alta. L.R. (5th) 1, 490 A.R. 327, 221 C.R.R. (2d) 198, 497 W.A.C. 327, 2010 CarswellAlta 2269, 2010 CarswellAlta 2270, 2010 SCC 55, [2011] 2 W.W.R. 442 (S.C.C.) — followed

*R. v. Kwok* (2008), 2008 CarswellOnt 2634 (Ont. C.J.) — referred to

*R. v. McNeice* (2010), 2010 BCSC 1544, 2010 CarswellBC 2935 (B.C. S.C.) — referred to



2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

*R. v. Morelli* (2010), [2010] 4 W.W.R. 193, 72 C.R. (6th) 208, (sub nom. *R. v. U.P.M.*) 399 N.R. 200, [2010] 1 S.C.R. 253, 207 C.R.R. (2d) 153, 252 C.C.C. (3d) 273, 316 D.L.R. (4th) 1, (sub nom. *R. v. U.P.M.*) 477 W.A.C. 1, (sub nom. *R. v. U.P.M.*) 346 Sask. R. 1, 2010 CarswellSask 150, 2010 CarswellSask 151, 2010 SCC 8 (S.C.C.) — followed

*R. v. Patrick* (2009), 190 C.R.R. (2d) 1, 2009 CarswellAlta 481, 2009 CarswellAlta 482, 2009 SCC 17, 242 C.C.C. (3d) 158, 304 D.L.R. (4th) 260, 4 Alta. L.R. (5th) 1, 387 N.R. 44, 454 A.R. 1, [2009] 1 S.C.R. 579, [2009] 5 W.W.R. 387, 64 C.R. (6th) 1 (S.C.C.) — considered

*R. v. Plant* (1993), 157 N.R. 321, [1993] 8 W.W.R. 287, 145 A.R. 104, 55 W.A.C. 104, 17 C.R.R. (2d) 297, 12 Alta. L.R. (3d) 305, 84 C.C.C. (3d) 203, [1993] 3 S.C.R. 281, 24 C.R. (4th) 47, 1993 CarswellAlta 94, 1993 CarswellAlta 566 (S.C.C.) — considered

*R. v. Spencer* (2009), 361 Sask. R. 1, 2009 SKQB 341, 2009 CarswellSask 905 (Sask. Q.B.) — referred to

*R. v. Tele-Mobile Co.* (2008), 2008 CarswellOnt 1588, 2008 CarswellOnt 1589, 2008 SCC 12, (sub nom. *Tele-Mobile Co. v. Ontario*) 372 N.R. 157, 55 C.R. (6th) 1, (sub nom. *Ontario v. Tele-Mobile Co.*) 229 C.C.C. (3d) 417, (sub nom. *Tele-Mobile Co. v. Ontario*) 235 O.A.C. 369, (sub nom. *Tele-Mobile Co. v. Ontario*) [2008] 1 S.C.R. 305, (sub nom. *R. v. Tele-Mobile Company (Telus Mobility)*) 92 O.R. (3d) 478 (note), (sub nom. *Ontario v. Tele-Mobile Co.*) 291 D.L.R. (4th) 193 (S.C.C.) — referred to

*R. v. Tessling* (2004), 326 N.R. 228 (Eng.), 326 N.R. 228 (Fr.), 192 O.A.C. 168, [2004] 3 S.C.R. 432, 2004 SCC 67, 2004 CarswellOnt 4351, 2004 CarswellOnt 4352, 189 C.C.C. (3d) 129, 244 D.L.R. (4th) 541, 75 O.R. (3d) 480 (note), 23 C.R. (6th) 207, 123 C.R.R. (2d) 257 (S.C.C.) — followed

#### Cases considered by *Ottobreit J.A.*:

*Canada (Director of Investigation & Research, Combines Investigation Branch) v. Southam Inc.* (1984), (sub nom. *Hunter v. Southam Inc.*) 11 D.L.R. (4th) 641, 33 Alta. L.R. (2d) 193, (sub nom. *Hunter v. Southam Inc.*) 55 A.R. 291, 27 B.L.R. 297, 41 C.R. (3d) 97, 84 D.T.C. 6467, (sub nom. *Hunter v. Southam Inc.*) 14 C.C.C. (3d) 97, (sub nom. *Director of Investigations & Research Combines Investigation Branch v. Southam Inc.*) [1984] 6 W.W.R. 577, 1984 CarswellAlta 121, 1984 CarswellAlta 415, (sub nom. *Hunter v. Southam Inc.*) [1984] 2 S.C.R. 145, (sub nom. *Hunter v. Southam Inc.*) 55 N.R. 241, (sub nom. *Hunter v. Southam Inc.*) 2 C.P.R. (3d) 1, (sub nom. *Hunter v. Southam Inc.*) 9 C.R.R. 355, 48 N.R. 320 (S.C.C.) — considered

*R. v. Ballendine* (2011), 271 C.C.C. (3d) 418, 2011 BCCA 221, 2011 CarswellBC 1069, 304 B.C.A.C. 20, 513 W.A.C. 20 (B.C. C.A.) — considered

*R. v. Brousseau* (2010), 2010 CarswellOnt 10252, 2010 ONSC 6753, 264 C.C.C. (3d) 562 (Ont. S.C.J.) — considered

*R. v. Chehil* (2009), 199 C.R.R. (2d) 343, 248 C.C.C. (3d) 370, 71 C.R. (6th) 55, 284 N.S.R. (2d) 130, 901 A.P.R. 130, 2009 CarswellNS 602, 2009 NSCA 111 (N.S. C.A.) — considered

*R. v. Cuttall* (2009), 203 C.R.R. (2d) 342, 247 C.C.C. (3d) 424, 2009 CarswellOnt 5896, 2009 ONCJ 471 (Ont. C.J.) — distinguished

*R. v. Gomboc* (2010), 328 D.L.R. (4th) 71, [2010] 3 S.C.R. 211, 263 C.C.C. (3d) 383, 79 C.R. (6th) 199, 408 N.R.

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

1, 34 Alta. L.R. (5th) 1, 490 A.R. 327, 221 C.R.R. (2d) 198, 497 W.A.C. 327, 2010 CarswellAlta 2269, 2010 CarswellAlta 2270, 2010 SCC 55, [2011] 2 W.W.R. 442 (S.C.C.) — followed

*R. v. Kwok* (2008), 2008 CarswellOnt 2634 (Ont. C.J.) — distinguished

*R. v. M. (A.)* (2008), 55 C.R. (6th) 314, 236 O.A.C. 267, 293 D.L.R. (4th) 187, 2008 SCC 19, 2008 CarswellOnt 2257, 2008 CarswellOnt 2258, 230 C.C.C. (3d) 377, 92 O.R. (3d) 398 (note), 373 N.R. 198, [2008] 1 S.C.R. 569 (S.C.C.) — considered

*R. v. McNeice* (2010), 2010 BCSC 1544, 2010 CarswellBC 2935 (B.C. S.C.) — considered

*R. v. Patrick* (2009), 190 C.R.R. (2d) 1, 2009 CarswellAlta 481, 2009 CarswellAlta 482, 2009 SCC 17, 242 C.C.C. (3d) 158, 304 D.L.R. (4th) 260, 4 Alta. L.R. (5th) 1, 387 N.R. 44, 454 A.R. 1, [2009] 1 S.C.R. 579, [2009] 5 W.W.R. 387, 64 C.R. (6th) 1 (S.C.C.) — followed

*R. v. Plant* (1993), 157 N.R. 321, [1993] 8 W.W.R. 287, 145 A.R. 104, 55 W.A.C. 104, 17 C.R.R. (2d) 297, 12 Alta. L.R. (3d) 305, 84 C.C.C. (3d) 203, [1993] 3 S.C.R. 281, 24 C.R. (4th) 47, 1993 CarswellAlta 94, 1993 CarswellAlta 566 (S.C.C.) — followed

*R. v. Tessling* (2004), 326 N.R. 228 (Eng.), 326 N.R. 228 (Fr.), 192 O.A.C. 168, [2004] 3 S.C.R. 432, 2004 SCC 67, 2004 CarswellOnt 4351, 2004 CarswellOnt 4352, 189 C.C.C. (3d) 129, 244 D.L.R. (4th) 541, 75 O.R. (3d) 480 (note), 23 C.R. (6th) 207, 123 C.R.R. (2d) 257 (S.C.C.) — referred to

*R. v. Vasic* (2009), 185 C.R.R. (2d) 286, 2009 CarswellOnt 846 (Ont. S.C.J.) — considered

*R. v. Ward* (2008), 2008 ONCJ 355, 2008 CarswellOnt 4728, 176 C.R.R. (2d) 90 (Ont. C.J.) — considered

*R. v. Weir* (1998), 213 A.R. 285, [1998] 8 W.W.R. 228, 1998 CarswellAlta 151, 59 Alta. L.R. (3d) 319, 1998 ABQB 56 (Alta. Q.B.) — referred to

*R. v. Wilson* (2009), 2009 CarswellOnt 2064 (Ont. S.C.J.) — considered

*United States v. Bynum* (2010), 604 F.3d 161 (U.S. C.A. 4th Cir.) — considered

*United States v. Maxwell* (1995), 42 M.J. 568 (U.S. A.F. Ct. Crim. App.) — referred to

*United States v. Perrine* (2008), 518 F.3d 1196 (U.S. C.A. 10th Cir.) — considered

*United States v. Stults* (2009), 575 F.3d 834 (U.S. C.A. 8th Cir.) — considered

#### Statutes considered by *Cameron J.A.*:

*Canadian Charter of Rights and Freedoms*, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11

Generally — referred to

s. 8 — considered

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

*Criminal Code*, R.S.C. 1985, c. C-46

- s. 163 — referred to
- s. 487.012 [en. 2004, c. 3, s. 7] — referred to
- s. 487.014 [en. 2004, c. 3, s. 7] — considered
- s. 487.014(1) [en. 2004, c. 3, s. 7] — considered

*Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01

- Pt. IV — referred to
- s. 29(2)(g) — considered
- s. 29(2)(g)(i) — considered
- s. 29(2)(g)(ii) — considered
- s. 29(2)(g)(iii) — considered

**Statutes considered by Ottenbreit J.A.:**

*Canadian Charter of Rights and Freedoms*, Part I of the Constitution Act, 1982, being Schedule B to the Canada Act 1982 (U.K.), 1982, c. 11

- Generally — referred to
- s. 7 — considered
- s. 8 — considered

*Criminal Code*, R.S.C. 1985, c. C-46

- s. 161 — referred to
- s. 163.1(3) [en. 1993, c. 46, s. 2] — referred to
- s. 163.1(4) [en. 1993, c. 46, s. 2] — referred to
- s. 163.1(4.1) [en. 2002, c. 13, s. 5(3)] — referred to
- s. 487.014 [en. 2004, c. 3, s. 7] — considered
- s. 487.014(1) [en. 2004, c. 3, s. 7] — considered

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

s. 675(1)(a) — considered

s. 675(1)(a)(i) — considered

s. 675(1)(b) — considered

*Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01

s. 29(2) — considered

s. 29(2)(g) — considered

*Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5

Generally — referred to

#### **Regulations considered by *Cameron J.A.*:**

*Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01

*Freedom of Information and Protection of Privacy Regulations*, R.R.S., c. F-22.01, Reg. 1

Generally — referred to

APPEAL from judgment reported at *R. v. Trapp* (2009), 344 Sask. R. 300, 2009 SKPC 109, 2009 CarswellSask 725 (Sask. Prov. Ct.), convicting accused of making available, accessing, and having in his possession child pornography.

#### ***Cameron J.A.*:**

1 I have had the advantage of reading the draft reasons for judgment of my colleague, Ottenbreit J.A., dismissing this appeal. I, too, would dismiss the appeal, but for somewhat different reasons.

2 My colleague has set out the background facts, so I need not recount them. At the heart of the case lies the information the police sought and obtained from SaskTel as the accused's Internet Service Provider. The information consisted of the IP Address SaskTel had assigned to him as of a specific date and time.

3 I am of the view the accused enjoyed a reasonable expectation of privacy in relation to this information, because the information was private and confidential, and because information of this nature is potentially capable of revealing much about the individual, and the online activity of the individual inside the home. Hence, I have concluded that the conduct of the police in obtaining the information from SaskTel constituted a search within the meaning of section 8 of the *Charter*. However, I have also concluded that the search was reasonable, and in consequence I, too, would dismiss the appeal.

4 I have come to these conclusions on the following bases, beginning with the governing framework of principle.

#### **1. The Framework of Principle Governing the Matter**

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

5 Section 8 of the *Charter* guarantees the right of everyone to be secure against *unreasonable* search or seizure. That being so, its principal purpose lies in protecting persons from unreasonable state intrusion upon their privacy or, expressed positively, to protect the person's *reasonable expectation of privacy* in relation to the state. This makes it necessary, when the section is invoked, to assess the person's interest in being left alone by the government against the government's interest in intruding upon the privacy of the person for the purpose of law enforcement: *Canada (Director of Investigation & Research, Combines Investigation Branch) v. Southam Inc.*, [1984] 2 S.C.R. 145 (S.C.C.).

6 This assessment, when the section is invoked in relation to police conduct in the course of a criminal investigation, entails a two step inquiry: (1) whether the conduct of the police constituted a "search" within the meaning of section 8 and, if so, (2) whether the search was reasonable: *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432 (S.C.C.).

### ***(1) The First Step of the Inquiry***

7 This step is governed by the following general principles, drawn from *Tessling's* case.

8 To begin with, the onus of establishing that a search has occurred is on the person who invokes the protection of the section. If the conduct of the police is shown to have intruded upon a reasonable expectation of privacy in the person, a "search" will have occurred. For this purpose, the person must enjoy a *subjective* expectation of privacy in the subject matter of the alleged search, and his or her expectation must be *objectively* reasonable. Otherwise there is no expectation of privacy and therefore no search.

9 A subjective expectation of privacy may be presumed to exist in some circumstances, but the objective reasonableness of that expectation must always be demonstrated on the basis of the totality of the circumstances.

10 In a case featuring allegedly confidential and private information about a person in the hands of a third party, the totality of the circumstances includes:

- the nature of the privacy interest asserted by the person;
- the precise nature of the subject matter of the alleged search;
- the relationship between the third party and the person;
- the legal framework governing disclosure of the information;
- the intrusiveness of the alleged search; and
- such other factors as may bear upon the strength or weakness of the expectation of privacy at issue.

11 When it comes to the *nature of the privacy interest* asserted by the person, it is necessary to bear in mind that privacy interests include personal privacy (concerning one's body and bodily integrity), territorial privacy (the places one occupies, such as the home or the workplace), and informational privacy (the information about self that one may or may not wish to have disclosed).

12 As for territorial privacy, Mr. Justice Binnie, who delivered the unanimous judgment of the Court in *Tessling's* case, observed that privacy in the home is of foremost concern:

22 The original notion of territorial privacy ("the house of everyone is to him as his castle and fortress": *Semayne's Case*, [1558-1774] All E.R. Rep. 62 (1604), at p. 63) developed into a more nuanced hierarchy protecting privacy

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

in the home, being the place where our most intimate and private activities are most likely to take place (*Evans*, [[1996] 1 S.C.R. 8], at para. 42; *R. v. Silveira*, [1995] 2 S.C.R. 297, at para. 140, *per* Cory J.: "[t]here is no place on earth where persons can have a greater expectation of privacy than within their 'dwelling-house'"; *R. v. Feeney*, [1997] 2 S.C.R. 13, at para. 43)....

13 With that, Justice Binnie turned to informational privacy and what it entails:

23 Beyond our bodies and the places where we live and work, however, lies the thorny question of how much information about ourselves and activities we are entitled to shield from the curious eyes of the state (*R. v. S.A.B.*, [2003] 2 S.C.R. 678, 2003 SCC 60)....Informational privacy has been defined as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others": A. F. Westin, *Privacy and Freedom* (1970), at p. 7. Its protection is predicated on

the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain ... as he sees fit.

(Report of a Task Force established jointly by Department of Communications/Department of Justice, *Privacy and Computers* (1972), at p. 13).

[Emphasis in S.C.R.]

14 It is one thing, of course, to define the notion of informational privacy in general terms, another to work with it in striking the balance between interests of the individual and those of the state. Recognizing this, Justice Binnie said:

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

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

[Emphasis in S.C.R.]

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

15 There is one other thing of note about all of this. Justice Binnie also explained that the various privacy interests may overlap:

24 The distinction between personal, territorial and informational privacy provides useful analytical tools, but of course in a given case, the privacy interest may overlap the categories. Here, for example, the privacy interest is essentially informational (i.e. about the respondent's activities) but it also implicates his territorial privacy because although the police did not actually enter his house, that is where the activities of interest to them took place.

16 In sum, then, this is the framework of principle governing the first step of the inquiry: whether, in the case of



2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

police conduct, the conduct constituted a search within the meaning of section 8. I should add, perhaps, that this is but a brief summary, and there are other cases with a further bearing upon the subject, including in particular *R. v. Plant*, [1993] 3 S.C.R. 281 (S.C.C.); *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579 (S.C.C.); and, most recently, *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211 (S.C.C.). For the moment, however, this will do.

## ***(2) The Second Step of the Inquiry***

17 This step is concerned with the reasonableness of a search. Accordingly, it is necessary to take this step only if the person who invoked section 8 establishes that the conduct of the police amounted to a search. In that event, the question is whether the search was reasonable and, in the case of a warrantless search, the Crown bears the burden of the demonstration. Two basic principles are at work in this context. The first is that a warrantless search, while capable of constituting a reasonable search, is presumptively unreasonable: *R. v. Collins*, [1987] 1 S.C.R. 265 (S.C.C.). The second is that, even so, a search is "reasonable" if (a) it is authorized by law; (b) the law is reasonable; and (c) the search is carried out in reasonable manner: *Collins*.

## **2. The Application of this Framework of Principle to the Present Case**

This, of course, entails conducting the two-step in inquiry referred to above.

### ***(1) Step One of the Inquiry.***

18 The question here is whether the accused made out a sufficient case to engage section 8. In other words, can he be taken to have established that the conduct of the police constituted a search within the meaning of the section?

19 This comes down to whether he enjoyed a reasonable expectation of privacy in the information sought and obtained by the police from SaskTel for the purposes of furthering their investigation and laying the groundwork for obtaining a search warrant — a warrant enabling them to search his home, seize his computer, and search the computer for evidence he accessed, possessed and made available child pornography contrary to section 163 of the *Criminal Code*.

20 The police sought and obtained from SaskTel information regarding the Internet Protocol Address it had assigned to him in relation to his access to the Internet. Whether he enjoyed a reasonable expectation of privacy in relation to this information reduces to this: Did he harbor a subjective expectation of privacy in that information, and if so, was his expectation objectively reasonable having regard for the totality of the circumstances?

21 I am satisfied this is an appropriate case in which to ascribe to him a subjective expectation of privacy in relation to this information, even though he did not testify to this. I say this having regard for the nature and quality of the information — a matter I shall come to shortly — and the relatively low threshold at work here. In principle, the point finds illustration in *R. v. Gomboc* (cited above).

22 The critical question, then, is whether his expectation of privacy in relation to this information may be seen to have been reasonable when viewed objectively in light of the totality of the circumstances and from the perspective of the reasonable and informed person concerned about the protection of privacy. As Justice Binnie observed in *R. v. Patrick* (cited above):

[14] ... Privacy analysis is laden with value judgments which are made from the independent perspective of the reasonable and informed person who is concerned about the long-term consequences of government action for the protection of privacy.



2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

[emphasis added]

With this in mind I turn to the totality of the circumstances, beginning with the nature of the privacy interest being asserted.

*(i) the nature of the privacy interest asserted by the accused*

23 For the most part, he asserted an informational privacy interest: one having to do with when and how and to what extent the information held by SaskTel as his Internet Service Provider was communicated to others. In a sense he also asserted a territorial privacy interest, claiming the information sought and obtained by the police touched upon his activity within his home.

24 In asserting these interests he suggested they were inextricably linked to his own use of his own computer in his own home, suggesting this served virtually in itself to demonstrate that he had a reasonable expectation of privacy in the subject matter of the alleged search: *R. v. Kwok*, [2008] O.J. No. 2414 (Ont. C.J.); *R. v. Cuttell*, 2009 ONCJ 471 (Ont. C.J.), 247 C.C.C. (3d) 424 (Ont. C.J.). I think the point is overdrawn in the sense at least that there is more to the analysis than this. But I do acknowledge the general idea that privacy and confidentiality are very much associated with the use and content of one's computer. The idea finds expression in the opening remarks of Mr. Justice Fish in *R. v. Morelli*, 2010 SCC 8, [2010] 1 S.C.R. 253 (S.C.C.), remarks with which I entirely agree:

2 It is difficult to imagine a search more intrusive, extensive, or invasive of one's privacy than the search and seizure of a personal computer.

3 First, police officers enter your home, take possession of your computer, and carry it off for examination in a place unknown and inaccessible to you. There, without supervision or constraint, they scour the entire contents of your hard drive: your emails sent and received; accompanying attachments; your personal notes and correspondence; your meetings and appointments; your medical and financial records; and all other saved documents that you have downloaded, copied, scanned, or created. The police scrutinize as well the electronic roadmap of your cybernetic peregrinations, where you have been and what you appear to have seen on the Internet — generally by design, but sometimes by accident.

25 As I say, I think the accused has overdrawn his point, inasmuch as there is more to the analysis than he suggests. Nevertheless, the point serves, first, to add to the understanding of the nature of informational privacy when it comes to personal computer use and, second, to buttress his assertion of territorial privacy in the sense, noted in *Tessling* at para. 24, that "although the police did not actually enter his house, that is where the activities of interest to them took place."

26 Beyond this lies a point of more specific significance in assessing the totality of the circumstances, namely the subject matter of the alleged search.

*(ii) the subject matter of the alleged search*

27 It is imperative that this be accurately identified. As remarked upon by Justice Binnie in *R. v. Patrick* (cited above):

29 It is essential at the outset to identify the subject matter of the alleged search: *Tessling* (at paras. 34 and 58). In *R. v. Kang-Brown*, 2006 ABCA 199, 210 C.C.C. (3d) 317, the Alberta Court of Appeal accepted the Crown's argument that the subject matter of the sniffer-dog search was the public airspace surrounding a traveler's bag. In this Court, the subject matter was found to be the contents within, and specifically the existence of narcotics (2008 SCC 18, [2008] 1 S.C.R. 456). The differing perspectives made a major contribution to a different result.

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

28 Mindful of this, I note that here the police requested SaskTel to provide them with "any information relating to the information on IP 207.47.225.82 on July 24, 2007 at 18:37 hrs. (local Saskatchewan time)."

29 It is important to the understanding of this request to place it in context. To begin with, the request was made of SaskTel in its capacity as an Internet Service Provider. As an Internet Service Provider, SaskTel is in the business of providing access to the Internet to computer owners who subscribe for this service and pay for it. Those who do so may access the Internet by means of either a "Dial Up" or "High Speed" service provided by SaskTel through its telephone lines. Each time the subscriber accesses the Internet in one or the other of these ways, or "goes online" so to speak, SaskTel assigns the subscriber a discrete Internet Protocol Address, or IP Address. This consists of a 30 bit number unique to SaskTel. If the subscriber goes online by way of the Dial Up service, SaskTel assigns an IP address each time the subscriber does so; and the number changes each time. If the subscriber goes online via the High Speed service, SaskTel again assigns the subscriber an IP address each time the subscriber does so, but the number remains largely constant.

30 Not surprisingly, perhaps, SaskTel maintains an electronically stored record of the IP addresses it assigns to each of its subscribers each time they access the Internet. How long it maintains this record we do not know. But we do know that for some period of time SaskTel is able to determine from this record on what day, and at what time during the day, one of its subscribers (or someone using the subscriber's Internet service), was online. It is able to do this with reference to the assigned IP Address. SaskTel also maintains electronically stored Customer Account records, containing the name and billing address and telephone number of each of its customers, together with a description of the services for which each has subscribed.

31 This, coupled with the knowledge the police had gained in their investigation up to the point of contacting SaskTel, serves to explain why the police requested SaskTel to provide them with any information it had regarding "IP Address 207.47.225.82 on July 24, 2007 at 18:37 hrs. (local Saskatchewan time)." It also serves to explain SaskTel's response. In response, SaskTel brought up its electronically stored IP Addresses and Customer Account records, and then informed the police that, as of this date and time, IP address 207.47.225.82 was assigned to Brian Trapp whose civic address for billing purpose was #90, 219 Grant Street, Saskatoon, Saskatchewan, and whose telephone number was 306-249-4610.[FN1]

32 This, then, is the information the police sought and obtained from SaskTel, which is to say this is "the information in question", and it is this information that formed "the subject matter of the alleged search."

33 That said, it remains to identify the import or quality of this information, having regard for the principle that section 8 protects a biographical core of personal information, including information tending to reveal intimate details of the lifestyle and personal choices of the individual.

34 We heard a good deal of argument about this, replete with all manner of analogy. Leaving aside the analogies, which are only distracting, counsel for the Attorney General contended that the information in question does not contain a biographical core of personal information, for it is merely "subscriber information" or "customer information." Or it is nothing more than "name, address, and telephone number information" published in the telephone directory and available in the public domain; or "tombstone-like" information. In support of this contention, counsel for the Attorney General cited a number of lower court decisions in which similar information was similarly characterized, including *R. v. McNeice*, 2010 BCSC 1544 (B.C. S.C.) and *R. v. Spencer*, 2009 SKQB 341, 361 Sask. R. 1 (Sask. Q.B.).

35 With respect I do not find these characterizations to be particularly helpful. The information that forms the subject matter of the alleged search is what it is. And it seems to me there is no need to label it. Either it contains a biographical core of personal information or it does not, and I think it is unhelpful to the determination of that issue to

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

label the information in some such way. Even worse, such labels are apt to skew the analysis. To label information of this kind as mere "subscriber information" or "customer information", or nothing but "name, address, and telephone number information", tends to obscure its true nature. I say this because these characterizations gloss over the significance of an IP address and what such an address, once identified with a particular individual, is capable of revealing about that individual, including the individual's online activity in the home.

36 Here, for example, the police were able to learn, once informed about the name of the person to whom SaskTel had assigned the IP address in question, that the accused, or likely the accused, was online at 6:37 pm on July 4, 2007 and logged onto the Gnutella network. This enabled them, in turn, to complete a history of his activity on that network. And apparently this is but the beginning of what someone might learn of another if supplied with the identity of the person to whom an IP address is assigned.

37 The point, at least at this stage of the inquiry, is not about what the police did, but rather about the *quality* of this kind of information, namely its potential to reveal much about the individual, and the individual's activity in the home.

38 True, people routinely disclose to others their names and addresses and telephone numbers, and routinely allow access to information about what goes on inside the home, but only for *some* purposes, *not for all*. The point was aptly made by Justice Fish in *R. v. Gomboc* (cited above).

[100] Every day, we allow access to information about the activities taking place inside our homes by a number of people, including those who deliver our mail, or repair things when they break, or supply us with fuel and electricity, or provide television, Internet and telephone services. Our consent to these "intrusions" into our privacy, and into our homes, is both necessary and conditional: necessary, because we would otherwise deprive ourselves of services nowadays considered essential; and conditional, because we permit access to our private information for the *sole, specific, and limited purpose of receiving those services*. [emphasis added]

[101] A necessary and conditional consent of this sort does not trump our reasonable expectation of privacy in the information to which access is afforded for such a limited and well-understood purpose. When we subscribe for cable services, we do not surrender our expectation of privacy in respect of what we access on the Internet, what we watch on our television sets, what we listen to on our radios, or what we send and receive by e-mail on our computers.

39 I quite agree that, when one subscribes for Internet access service, one does not surrender one's expectation of privacy regarding what one chooses to access on the Internet. The point finds reinforcement in the following remarks of Justice Sopinka in *R. v. Plant* at p. 292 (cited above):

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*, [[1988] 2 S.C.R. 417], 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.

[emphasis added]

40 In sum, I am of the opinion the whole of the above considerations (including in particular those having to do with the nature and quality of the information in question), militate strongly in favor of an objectively reasonable

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

expectation of privacy in relation to that information and, hence, the subject matter of the alleged search.

41 This, of course, is but the beginning of the inquiry. The remaining circumstances have to be considered, including the fact the information in question was in the hands of a third party, namely SaskTel, and was under its control. This brings me to the relationship between SaskTel and the accused and, more particularly, to how SaskTel was to treat information of this kind and what authority it had to disclose such information to others. Naturally, the broader that authority, the narrower becomes the expectation of privacy, and *vice versa*.

*(iii) the relationship between SaskTel and the accused*

42 SaskTel provided the accused with telephone, Internet, and cable television service. It did so in accordance with the "General Terms of Service" agreed to by SaskTel and its customers. The "General Terms of Service" include the following provisions:

69.1 All information which SaskTel has about the customer is confidential except:

- (a) the customer's name, address and telephone number listed in the SaskTel telephone directory, *and*
- (b) the customer's name, address, and telephone number available through directory assistance.

69.2 Customers may request that their name, address and telephone number:

- (a) not be published, in which case they will not be listed in any SaskTel directory and will not be available through directory assistance, *or*
- (b) not be listed in any SaskTel telephone directory but still be made available through directory assistance....

\*\*\*

69.4 Unless a Customer provides express consent or disclosure pursuant to legal power, all information kept by SaskTel regarding the customer, other than the customer's name, address and listed telephone number, is confidential and may not be disclosed by SaskTel to anyone other than:

- (a) the customer
- (b) an agent, who in the reasonable judgement of SaskTel is seeking the information on behalf of the customer,

\*\*\*

- (f) a public authority or agent of a public authority, if in the reasonable judgement of SaskTel it appears that there is imminent danger to life or property which could be avoided or minimized by disclosure of the information.

\*\*\*

69.5 Despite the restrictions in item 69.4, SaskTel may disclose confidential customer information if:



2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

(a) the customer provides written consent,

(b) SaskTel is ordered to disclose the information by a court or administrative tribunal of competent jurisdiction, *or*

(c) SaskTel is otherwise legally empowered to disclose the information.

43 To the extent these provisions bear upon SaskTel's contractual authority to disclose to others the name, address, and telephone number of a subscriber, I regard them as largely irrelevant, given what I have had to say about information of this sort, contrasted with information of the nature and quality of the information in question.

44 That said, I am of the opinion these provisions are generally supportive of the accused's claim to an objectively reasonable expectation of privacy in the information in question and, therefore, the subject matter of the alleged search. There are two reasons for this. First, these provisions rendered the information "confidential". Second, they imposed an obligation upon SaskTel not to disclose such information to others except on the narrow authority specified in article 69.5, namely with consent, or pursuant to an order, or as "otherwise legally empowered."

45 Of these three, only the last is relevant to this case. It is found in clause (c) of article 69.5. I think this clause tends to weaken the reasonable expectation of privacy under consideration but not appreciably. I say that for the reasons that follow.

46 To begin with this clause states in effect that, despite the restrictions mentioned in article 69.4, SaskTel "may" disclose to others confidential information if "otherwise legally empowered" to do so. This suggests SaskTel cannot divulge confidential information pertaining to its Internet access subscribers in the absence of some external legal authority permitting it to do so. It also suggests that, even when such authority exists, SaskTel retains the discretionary power to disclose or not disclose such information.

47 On what basis SaskTel might exercise this discretion, having regard for the whole of the provisions of the "General Terms of Service" bearing upon confidentiality and disclosure, is debatable. But the reasonable person might well think that SaskTel does not enjoy an unfettered discretion to divulge confidential information to others — unfettered, that is, beyond the prerequisite of being "legally empowered" to do so. Otherwise, the information loses much if not all of its confidential character. And the element of confidentiality in the relationship is substantially compromised. So, the reasonable person might well think that SaskTel would be highly circumspect when it comes to divulging to others confidential information of the nature and quality of the information in question. This is why I say that, while clause (c) of article 69.5 of the "General Terms of Service" tends to weaken the objective reasonableness of the accused's expectation of privacy in relation to the information in question, it does not do so appreciably.

48 However, I recognize that there may be an indication to the contrary in the specific context in which SaskTel is "otherwise legally empowered" to disclose confidential information to others, particularly the police. And it is this to which I now turn.

*(iv) the legal power of SaskTel to disclose to the police*

49 SaskTel is empowered by statute to disclose personal information about its subscribers to prescribed law enforcement agencies and investigative bodies. Rather ironically, perhaps, this power is found in a statute devoted in major part to the privacy of the individual and the protection of private information. The power is found in *The Freedom of Information and Protection of Privacy Act*, S.S. 1990-91, c. F-22.01, and more specifically in subsection 29(2)(g) of the *Act*, which reads thus:

29(2) Subject to any other Act or regulation, personal information in the possession or under the control of a

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

government institution may be disclosed

...

(g) to a prescribed law enforcement agency or a prescribed investigative body:

(i) on the request of the law enforcement agency or investigative body;

(ii) for the purpose of enforcing a law of Canada or a province or territory or carrying out a lawful investigation; and

(iii) if any prescribed requirements are met.

50 Before turning to how this subsection affects the expectation of privacy under consideration, I should like to point out that the constitutional validity of the subsection is not in issue. We must therefore assume that it is constitutionally sound as it stands. I should also like to point out, first, that SaskTel is a Crown Corporation and is identified as such in *The Freedom of Information and Protection of Privacy Regulations* as "a government institution"; second, that the Saskatoon Police Service is a "prescribed law enforcement agency" under the *Regulations*; and, third, that the *Regulations* contain no "prescribed requirements" as contemplated by clause (iii) of subsection 29(2)(g), at least not in relation to a request of SaskTel by a law enforcement agency.

51 That aside, it was suggested in argument that the police sought and obtained the information in question on the authority of subsection 29(2)(g). I do not agree. True, the police sought the information with the subsection *in mind*, but they did not do so on the *authority* of it in the strict sense. The subsection does not confer police power. Rather it confers authority on government institutions, SaskTel included, to disclose "personal information" about others to the police for the purpose of furthering a lawful police investigation.

52 With that, I turn to the significance of subsection 29(2)(g), and the authority it confers on SaskTel to disclose private information to the police (i) on request, (ii) for the purpose of a lawful police investigation, and (iii) in accordance with prescribed requirements. Since in this instance there are no prescribed requirements, as contemplated by clause (iii) of the subsection, it appears the only strictures on the exercise of this authority are those mentioned in clauses (i) and (ii) of the subsection, and those that may flow by implication from a fully contextual interpretation of the subsection, including the purpose of Part IV of the *Act*, which is expressly dedicated to protection of privacy. Either that, or presumably such strictures as exist must be found elsewhere as, for example, in statutory provisions specific to the institution, or in its contractual or other obligations.

53 In any event, since the subsection states in effect that SaskTel "may" on request of the police disclose private information about others to the police for the purpose of a lawful investigation, the subsection appears to confer *discretionary authority* to do so. That is the usual implication of employing the word "may" in place of "shall", implying that the holder of the authority can lawfully decide whether or not to exercise that authority.

54 It is unnecessary to be definitive about this, however, for we are here concerned only with what a reasonable person, alert to the provisions of articles 69.4 and 69.5 of the "General Terms of Service" and subsection 29(2)(g) of the *Act*, might reasonably expect of SaskTel, as an Internet Service Provider, when asked by the police to disclose to them *confidential* and *private* information of the nature and quality of the information in question. That such information is *confidential* is clear from the "General Terms of Service." That it is *private* is clear from the *Act*.

55 It seems to me that a reasonable person, mindful of the fact such confidential and private information is potentially capable of revealing much about the online activity of the individual in the home, and mindful, too, of the obligations of SaskTel to its subscribers, might reasonably expect SaskTel to exercise a meaningful measure of in-

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

dependent and informed judgment before voluntarily disclosing such information to the police. This is especially so, I might add, of the reasonable and informed person concerned about the long-term consequences of government action for the protection of privacy.

56 It appears that other Internet Service Providers, sensitive to the quality of this kind of information, require a search warrant before disclosing such information to the police. (See *R. v. Cuttell*, cited above). We do not know whether SaskTel, as an Internet Service Provider, has adopted any policy in this regard. All we know is that, if it has done so, the policy does not find expression in the "General Terms of Service", and that in this instance SaskTel complied with the request of the police without suggesting the police might obtain a search warrant or an order of the court requiring production of the information. It might be noted that such "production orders" may be obtained on *ex parte* application under section 487.012 of the *Criminal Code* if the police have reasonable and probable grounds to believe an offence has been committed, or is suspected of being committed, and the person from whom production is sought is not implicated and is in possession of documents or data affording evidence of the commission of the offence.

57 On the whole, my point is two-fold. First, the reasonable person might reasonably expect SaskTel, as an Internet Service Provider, to exercise a meaningful measure of independent and informed judgment before disclosing information of the kind in question to the police on request. Second, it is not beyond the pale to suppose that in circumstances such as these a reasonable and informed person, concerned about the long-term consequences of the actions of government institutions for the protection of privacy, might expect SaskTel to suggest to the police that a production order might be appropriate having regard for the fact information such as this is both confidential and private, and is capable of revealing much about the individual and the individual's online activity in the home. I do not mean to imply this is necessarily so, but I do think it is not beyond the pale to suppose that a reasonable and informed person, thus concerned, might see the matter in this way.

58 Having regard for the foregoing, it seems to me that the combined effect of clause (c) of article 69.5 of the "General Terms of Service" and paragraph (g) of subsection 29(2) of the *Act*, serves to some extent to diminish the reasonable expectation of privacy in issue but does not serve to negate it. In my judgment it would take more than this to negate an objectively reasonable expectation of privacy in relation to information of the nature and quality of the information in question.

59 That, then, brings me to the intrusiveness of the alleged search and such other factors as may bear upon the strength or weakness of the expectation of privacy under consideration.

*(v) the intrusiveness of the alleged search*

60 Obviously, the alleged search occurred on the premises of SaskTel. And since the information in question was in its hands as a third party, and all the police did was request SaskTel to voluntarily disclose it to them, the alleged search cannot on the face of it be said to be anything but minimally intrusive, if that.

61 Beneath the surface of it, however, lies the subject matter of the alleged search, namely the information in question and what it was capable of revealing about the accused, including his online activity initiated in his home. In this sense, the alleged search, while unobtrusive on the surface of it, was nevertheless distinctly intrusive of his privacy, which is to say his informational privacy in particular and his territorial privacy as well. As mentioned above, while the police did not actually enter his home, this is where the activities of interest to them took place.

62 On this view of the relative intrusiveness of the alleged search, I conclude that there is little here to appreciably weaken the accused's claim to an objectively reasonable expectation of privacy in the information in question.

63 As for such other factors as may bear upon the matter, I note that there was a time when the seriousness of the



2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

offence under investigation had a bearing. But this is no longer so. As Justice Binnie observed on behalf of the Court in *Tessling's* case:

64 I wish to add one further observation. In *Plant*, Sopinka J. listed the seriousness of the offence as a factor in the "balance" sought to be achieved in s. 8 of the *Charter* (p. 295). Undoubtedly the "seriousness of the offence" has a role to play in striking "the balance", but I do not think that it is a factor in determining whether the respondent did or did not have a reasonable expectation of privacy in the heat distribution patterns on the outside of his house. Rather, it may more logically arise at the stage the court considers whether a particular search was reasonable, or whether the evidence obtained by an unreasonable search may be admitted into evidence under s. 24(2) of the *Charter*.

64 On the totality of the circumstances, then, I am satisfied that the accused enjoyed a reasonable expectation of privacy in relation to the subject matter of the alleged search and that the police intruded upon his privacy when it sought and obtained the information in question from SaskTel. That being so, I am satisfied a search occurred within the meaning of section 8.

65 That, then, takes me to the reasonableness of the search and the second step of the inquiry.

## ***(2) Step Two of the Inquiry***

66 The first question here is whether the search was authorized by law. The police may be taken to have conducted the search on the authority of section 487.014 of the *Criminal Code*. In general, this section allows a police officer, without a "production order", to request a person to voluntarily provide information about another, provided the person of whom the request is made is not prohibited by law from disclosing such information.

67 This section was enacted in 2004 in the context of the enactment, among others, of section 487.012. Section 487.012 empowers the courts to make "production orders" requiring a person (other than a person under investigation), to produce documents and data to peace officers or other public officers if there are reasonable grounds to believe an offence has been committed (or is suspected of having been committed), and the documents or data will afford evidence thereof. Thus subsection 487.014(1) reads as follows:

**487.014(1) Power of peace officer** — For greater certainty, no production order is necessary for a peace officer or public officer enforcing or administering this or any other Act of Parliament to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing.

68 I note at the outset that the constitutional validity of this subsection is not in issue in this case. The constitutional validity of the subsection was neither challenged, nor argued. We must therefore assume the subsection is constitutionally sound. I also note that these are relatively new provisions, and as far as we know they have not been interpreted, either standing alone or alongside the *Charter*. The Supreme Court of Canada had occasion recently to consider the provisions of which section 487.014 forms a part, namely those pertaining to production orders: *R. v. Tele-Mobile Co.*, 2008 SCC 12, [2008] 1 S.C.R. 305 (S.C.C.). But the issue there was a particularly narrow one (whether the cost associated with responding to such an order might be recovered), so the case did not engage section 487.014.

69 That said, the section is quite straightforward. The express language of the section may carry with it some implied limitations, but even so I am of the view that in this case the police were able to rely on the section to seek and obtain from SaskTel the information in question. I say this for two reasons.

70 First, the police had reasonable and probable grounds to believe that an offence or offences against section 163 of the *Criminal Code* had been committed and that SaskTel was in possession of information affording evidence

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

thereof. I do not say this was necessary, as a matter of law, to enable the police to act on section 487.014. I only state this to be the fact. But should the law come to require this, as a prerequisite to acting on the section, the requirement was met. Second, the police had every reason to believe that SaskTel was not prohibited by law from disclosing this information. Indeed, the police expressly referred to section 29(2)(g) of *The Freedom of Information and Protection of Privacy Act* in requesting of SaskTel to disclose the information. Again I merely state this to be the fact. And, of course, SaskTel voluntarily released the information on the request of the police.

71 I conclude from this that the search was authorized by law, that the law is reasonable in the sense it is here assumed to be constitutionally sound, and that the manner in which the search was conducted was reasonable.

72 For the whole of these reasons, then, I too would dismiss the appeal.

**Jackson J.A.:**

I concur:

**Ottobreit J.A.:**

## **I. Introduction**

73 Brian Arnold Trapp ("Mr. Trapp") appeals from his conviction in the Provincial Court on November 5, 2009 on the following charges:

Count 1. On or about the 24<sup>th</sup> day of July, A.D. 2007, at or near Saskatoon, Saskatchewan did make available child pornography, contrary to section 163.1(3) of the *Criminal Code* ("the Code").

Count 2. On or about the 24<sup>th</sup> day of July, A.D. 2007, at or near Saskatoon, Saskatchewan did access child pornography, contrary to section 163.1(4.1) of the *Code*.

Count 3. Between the 24<sup>th</sup> day of July, A.D. 2007, and the 28<sup>th</sup> day of August, A.D. 2007, at or near Saskatoon, Saskatchewan did have in his possession child pornography, contrary to section 163.1(4) of the *Code*.

Count 4. On or about the 28<sup>th</sup> day of August, A.D. 2007, at or near Saskatoon, Saskatchewan did have in his possession child pornography, contrary to section 163.1(4) of the *Code*.

74 On each of the charges, Mr. Trapp received a sentence of 13 months incarceration plus three years probation, a three-year s. 161 order, a DNA order and a 20-year sex offender registry order. The matter proceeded in two stages; first a *Charter* application on which Mr. Trapp was unsuccessful and then the trial proper. Both proceeded on an agreed statement of facts.

## **II. Evidence and Background**

75 Constable Shepherd ("Shepherd") was a member of the Saskatoon Police Service. She had been trained as an undercover investigator monitoring peer-to-peer file-sharing on the Internet to determine if any users recently had child pornography on their computers and were trading that child pornography with other users. She was conducting an undercover investigation on the Gnutella Peer-to-Peer Network using publically available peer-to-peer client software. This network can be accessed using file sharing software such as Limewire. The Gnutella software when installed and running allows the user to search for pictures, movies and other files by entering descriptive text such as search terms. These terms are typically processed by a host computer based on the information about the file which has

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

been sent by individual users.

76 During the installation of the Gnutella client software, various settings are established which configure that computer to share files. Typically, a setting establishes the location of one or more selected directories or folders whose contents (files) are made available to other Gnutella users to download if they establish a one-to-one connection with that computer. This location is commonly referred to as a shared folder. A setting on the computer controls whether or not other users of the network can obtain a list of the files being shared by that computer on the network.

77 Shepherd was searching for images or videos of child pornography using key words known to be associated with these types of files. A search of the Gnutella Network would return to her a list of images and videos that had the keyword in the title along with their respective SHA-1 hash values. The SHA-1 hash value is a mathematical fingerprint which summarizes a number of identified data on a digital image. Every digital image has a consistent hash value unless it is altered. Shepherd would compare the returned list of SHA-1 values to the police database of known child pornography to determine which files are known to be child pornography. Once a specific file was identified as child pornography, Shepherd would begin downloading the file. While the file was being downloaded, the client software would display a list of candidates that were offering that file along with their respective internet protocol (IP) addresses. The IP addresses listed were checked through GnUC software developed by another police force as well as publically available software to determine their physical location. If one of the computers supplying a segment of requested child pornography was determined to be in her target area, Shepherd would browse that computer's shared folder by initiating one-on-one direct line between the undercover police computer and that user's computer. Browsing the user's shared folder allowed Shepherd to see all the files of that user being shared on the network.

78 Shepherd proceeded with her investigation of Mr. Trapp step by step as follows:

1. On the evening of July 24, 2007 Shepherd logged on to the Gnutella Network.
2. She then browsed the network for the purpose of determining whether anyone in Saskatchewan had files containing child pornography available for sharing on the network.
3. At 6:37 that evening (or at 18:37 hrs. as she put it), she discovered that a computer with the IP address 207.47.225.82, was logged on to the Gnutella network.
4. She then connected with that computer, browsed its shared file folder or folders, and discovered that they contained what she suspected were child pornography files available to others on the network.
5. With that, she downloaded and viewed a selection of the video and image files contained in the shared folder or folders, compared them to known child pornography files, and concluded that the folder or folders did indeed contain child pornography files.
6. She then generated an "IP History" for IP 207.47.225.82 by means of a software program available to the police for that purpose. The history showed that on July 24, 2007, as well as on several other occasions, the user of the computer assigned this IP address had logged on to the Gnutella network as a download candidate for files known to the police to contain child pornography.
7. She then logged on to a public website, DnsStuff.com, for the purpose of identifying the Internet Service Provider ("ISP") that had assigned IP 207.47.225.82. The ISP was shown to be SaskTel.
8. She then faxed SaskTel Security for information pertaining to this IP address.

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

9. More specifically, according to the documents filed by the prosecutor in the court below (Tab # 3 of the Binder marked as Exhibit P 1), she faxed a letter from the Saskatoon Police Service to SaskTel Security. The letter contained an official request, made under s. 29.2 of *The Freedom of Information and Protection of Privacy Act* ("*FIPPA*"), S.S. 1990-91, c. F-22.01 for "any information relating to the information on IP 207.47.225.82 on July 24, 2007 at 18:37 hrs. (local Saskatchewan time.)" This request was expressed to be made in conjunction with "an ongoing investigation."

10. In response, SaskTel faxed Shepherd informing her that, as of 18:34 hrs. on July 24, IP 207.47.225.82 "resolved to Brian Trapp." Attached to the fax was a copy of SaskTel's "Account Information" pertaining to Brian Trapp. The "Account Information" contained his civic address, #90, 219 Grant St. Saskatoon SK, and the services he had subscribed for, namely

- SaskTel Highspeed and Dialup Internet service (including his telephone number).
- Sasknet E-mail (including his e-mail address and login name).
- SaskTel Mobility phone service (including his cell phone number).
- SaskTel Max cable television service (including the programming he had subscribed for).

79 Of the whole of the information Shepherd obtained from SaskTel, the information vital for the purposes of the police investigation and to obtaining the search warrant consisted of the following:

- that as of 18:37 hrs. on July 24, SaskTel had assigned IP 207.47.225.82 to a computer connected to the internet by means of the internet service provided by SaskTel to a person named Brian Trapp and
- that, according to SaskTel's records, Brian Trapp, whose telephone number was 306-249-4610, lived at #90, 219 Grant Street, Saskatoon, Saskatchewan ("the Information").

The Information served to inform the police that, at that hour on that date, a person in possession of a computer with access to the internet through the internet service provided by SaskTel to Brian Trapp at #90, 219 Grant Street, Saskatoon, Saskatchewan had been online using IP 207.47.225.82.

80 After Shepherd obtained the Information from SaskTel, she was able to obtain from SGI his date of birth, his PIC number, information on the vehicles registered in his name, and a physical description. She was also able to locate the name of Mr. Trapp's employer. On August 21, 2007, Shepherd generated a second IP history report for Mr. Trapp's IP address showing that it had been logged five additional times as a download candidate between July 25, 2007 and July 26, 2007.

81 On August 23, 2007, a search warrant incorporating the Information provided by SaskTel was issued for the residence of Mr. Trapp at #90 - 219 Grant Street, Saskatoon, Saskatchewan. Once at the residence, Shepherd used a laptop computer to check for a wireless connection in the area and determined that there was none. A computer was seized in a bedroom at the residence. Upon checking the computer's desktop, Shepherd found icons of Limewire, BitLord and BitTorrent which are all file-sharing programs. Mr. Trapp, in a statement given to the police, admitted that he was the only one who used the computer. He declined to say anything about downloads of any movies or images, although he did admit he used Limewire to download files. He initially indicated that he turned the file-sharing function of his computer off, although when confronted with the fact that his computer was set to file share, he indicated that someone must have turned it on. He indicated that when he sees a file involving child pornography that he immediately deletes it. An examination of Mr. Trapp's computer by Sgt. Closson, a forensic computer analyst, confirmed that child pornography was located in Mr. Trapp's computer in the shared folder in Limewire.

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

Mr. Trapp's Limewire was set up so that Mr. Trapp could share his files while searching but not share when he was not searching.

82 The Crown tendered, in their brief on the *Charter* application, part of the General Terms of Service ("Terms of Service") to which every subscriber with SaskTel implicitly agrees. The Crown highlighted Article 57.1 of the Terms of Service, "Restrictions on Use of Telephone Services or Other SaskTel Services" which are the obligations of SaskTel customers upon contracting with SaskTel. Article 57.1 reads as follows:

57.1 Customers are responsible for ensuring that the services provided by them to SaskTel are not used:

(a) *for an illegal purpose,*

(b) *in an illegal manner,*

(c) to make annoying or offensive calls including but not limited to electronic mail and facsimile transmissions, or

(d) in any way which prevents other customers from fairly and proportionately using services provided by SaskTel.

Other portions of the Terms of Service, Articles 69.1, 69.2, 69.4 and 69.5, read as follows:

69.1 All information which SaskTel has about the customer is confidential except:

(a) the customer's name, address and telephone number listed in the SaskTel telephone directory, *and*

(b) the customer's name, address and telephone number available through directory assistance.

69.2 Customers may request that their name, address and telephone number:

(a) not be published, in which case they will not be listed in any SaskTel telephone directory and will not be available through directory assistance, *or*

(b) not be listed in any SaskTel telephone directory but still be made available through directory assistance.

SaskTel will charge customers for these services as per Tariff Item 160.10 (Telephone Directory Service).

69.4 Unless a Customer provides express consent or disclosure pursuant to legal power, all information kept by SaskTel regarding the customer, other than the customer's name, address and listed telephone number, is confidential and may not be disclosed by SaskTel to anyone other than:

(a) the customer,

(b) an agent who, in the reasonable judgement of SaskTel, is seeking the information on behalf of the customer,

\*\*\*



2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

(f) a public authority or agent of a public authority, if in the reasonable judgement of SaskTel it appears that there is imminent danger to life or property which could be avoided or minimized by disclosure of the information....

69.5 Despite the restrictions in Item 69.4, SaskTel may disclose confidential customer information if:

(a) the customer provides written consent,

(b) SaskTel is ordered to disclose the information by a court or administrative tribunal of competent jurisdiction, *or*

(c) SaskTel is otherwise legally empowered to disclose the information.

In its brief and in oral argument in the Court below, the Crown asserted that Mr. Trapp's name, address and telephone number appeared at p. 462 of the Saskatoon telephone directory. This was not denied by Mr. Trapp.

### III. Decision of the Trial Judge

83 In the court below, Mr. Trapp made a *Charter* application to exclude the evidence obtained pursuant to the search warrant covering Mr. Trapp's residence on the basis that the warrant could not have been obtained without Mr. Trapp's name and address which information was improperly obtained. Mr. Trapp argued that the use by the police of s. 29(2)(g) of *FIPPA* had infringed on his s. 7 *Charter* rights and additionally that the relevant portions of the *FIPPA* subsection were too vague. Mr. Trapp also alleged that pursuant to s. 8 of the *Charter*, his privacy rights had been infringed by the use of the *FIPPA* provision.

84 The Provincial Court judge determined that s. 29(2) of *FIPPA* and its regulations had sufficient clarity and precision for the accused and investigators to be properly apprised of their legal status to utilize it. He determined that the manner in which the police conducted that aspect of the investigation did not violate Mr. Trapp's s. 7 *Charter* rights. The Provincial Court judge also found that Mr. Trapp's reasonable expectation of privacy and security under s. 8 of the *Charter* and his right to informational privacy was not infringed by the conduct of the police during the course of the investigation because it occurred in accordance with s. 29(2)(g) of *FIPPA*. He dismissed the accused's *Charter* application. In due course, a conviction was entered.

### IV. The Parties' Positions

85 Mr. Trapp argues that there is a reasonable expectation of privacy when he is surfing the internet and that this expectation of privacy was breached by the police obtaining from SaskTel account information relative to the IP address it had assigned to the computer that was logged on to the internet at 18:37 hours on July 24, 2007. He argues that the Information, which was incorporated into the Information to Obtain Search Warrant for his home, tended to reveal intimate details of his lifestyle and personal choices and thus required a warrant. Mr. Trapp argues that the Provincial Court judge erred in concluding that he had no reasonable expectation of privacy in the Information and that there was no s. 8 *Charter* breach.

86 In support of his argument, Mr. Trapp proffered the case of *United States v. Maxwell*, 42 M.J. 568 (U.S. A.F. Ct. Crim. App. 1995), and *R. v. Weir*, 1998 ABQB 56, [1998] 8 W.W.R. 228 (Alta. Q.B.), both dealing with the expectation of privacy regarding E-mail. He also cited *R. v. Kwok*, [2008] O.J. No. 2414 (Ont. C.J.), and *R. v. Cuttell*, 2009 ONCJ 471, 247 C.C.C. (3d) 424 (Ont. C.J.), for the proposition that disclosures by companies of the names and addresses of internet customers would tend to disclose intimate details of lifestyle and choices and was a breach of privacy under s. 8 of the *Charter*.

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

87 The Crown argues that there is no reasonable expectation of privacy in the Information in these circumstances. It argues that subscriber information is not acquired biographical information within the meaning of *R. v. Plant*, [1993] 3 S.C.R. 281 (S.C.C.), and in any event, there is in these circumstances no subjective and definitely no objective expectation of privacy. The Crown argues that the contractual language in Article 57.1 demonstrates that, in the ongoing commercial relationship between SaskTel and Mr. Trapp, the ISP expressly disallows confidentiality and information relating to criminal activity. Moreover, s. 29(2) of *FIPPA* permits disclosure of that kind of information to police with certain prescribed law enforcement purposes. The Crown argues that the statutory provisions in *FIPPA* and the standard contractual language found in every SaskTel customer agreement militate against a finding that Mr. Trapp has an objectively reasonable expectation of privacy in the personal information gleaned from his IP address.

## V. Jurisdiction and the Standard of Appellate Review

88 The jurisdiction of this Court is set forth in s. 675(1)(a) and (b) of the *Criminal Code*. This appeal is taken in exercise of the right of appeal conferred by s. 675(1)(a)(i) and is taken on the primary ground that the trial judge erred in law in holding that the police had not violated s. 8 of the *Charter* in obtaining the Information pursuant to s.29(2) of *The Freedom of Information and Protection of Privacy Act*. Mr. Trapp's argument is that the judge erred in law in admitting into evidence the information the police obtained from SaskTel, which formed an indispensable part of the foundation for obtaining the search warrant and thus an indispensable part of the foundation for the conviction. In this case, the facts are not in dispute. The sole ground of appeal involves the consideration of the application of the *Charter*. It is therefore a question of law and the standard of review: correctness is not in dispute.

## VI. Analysis

### A. Introduction

89 It is important at the outset to state what this appeal is not about. It is not about any of the investigative steps taken by Shepherd except the step she took to obtain the information she requested from SaskTel as an ISP. More specifically, the appeal is not about the investigative practices employed by Shepherd in gaining access through the Gnutella Network to the shared folder's on Mr. Trapp's computer, or in downloading files stored in the shared folders, or in identifying the content of the files including child pornography, or in tracing the history of the use of the computer in relation to downloading child pornography. None of this was contested. Nor was there any evidence to suggest that Shepherd as part of her initial investigation accessed, or might have been able to access in Mr. Trapp's computer, any but the files contained in these shared folders. In this case, Mr. Trapp opened the door to his computer and, more specifically, to his shared files to other users of the Gnutella Network and invited them to upload files. It was through that open door that Shepherd was able to access the content of Mr. Trapp's computer that he made available.

90 The core of Mr. Trapp's argument is that there is an informational privacy right to the Information which SaskTel provided to the police using the provisions of *FIPPA*. The discrete issue on this appeal is whether or not the request by Shepherd for information at SaskTel using *FIPPA* is an unreasonable search and seizure, thereby violating Mr. Trapp's s. 8 *Charter* rights. For the reasons hereinafter set forth, I conclude that it is not a search and seizure.

### B. General Principles

91 Section 8 of the *Charter* provides "[e]veryone has the right to be secure against unreasonable search and seizure." The heart of this protection is an entitlement to a reasonable expectation of privacy.

92 Claims to privacy must be balanced against other societal needs including effective law enforcement. Dickson J. (as he then was) in *Canada (Director of Investigation & Research, Combines Investigation Branch) v. Southam Inc.*, [1984] 2 S.C.R. 145 (S.C.C.) framed a reasonable expectation of privacy as follows at pp. 159-160:



2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

The guarantee of security from unreasonable search and seizure only protects the reasonable expectation. This limitation on the right guaranteed by section 8 whether it is expressed negatively as freedom from "unreasonable" search and seizure, or positively as an entitlement to any "reasonable" expectation of privacy indicates 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 goal notably those of law enforcement.

93 In *R. v. Gomboc*, 2010 SCC 55, [2010] 3 S.C.R. 211 (S.C.C.), Deschamps J. at para. 18 describes the general analytical approach to determining whether a reasonable expectation of privacy exists:

[18] In *R. v. Edwards*, [1996] 1 S.C.R. 128, a majority of this Court held that a "reasonable expectation of privacy is to be determined on the basis of the totality of the circumstances" (para. 45). In subsequent cases, the reasonable expectation of privacy analysis proceeded in two steps, asking whether the accused had a subjective expectation of privacy and whether that expectation of privacy was objectively reasonable (*R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432, at para. 19; *R. v. Kang-Brown*, 2008 SCC 18, [2008] 1 S.C.R. 456; and *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579).

[23] ... I reiterate before undertaking that analysis that context is crucial and that reasonable expectation of privacy is assessed in the totality of the circumstances.

94 Generally three types of privacy interests receive constitutional protection, namely, (1) personal privacy; (2) territorial privacy; and (3) informational privacy (*R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432 (S.C.C.) at paras. 25 and 42) but these categories do not exist in isolation and sometimes overlap.

95 Deschamps J. at paras. 48-49 of *Gomboc* states:

48 Also noteworthy here is that the home itself was never directly the object of a search. The location where the search took place was not the home but the transformer box where the power lines entering the home could be accessed. After some confusion in the courts below about whether the transformer was located on Mr. Gomboc's property, it was common ground before this Court that it was not. Accordingly, no direct territorial privacy interest is engaged in this case.

49 Recent cases have recognized overlapping informational and territorial privacy when activities suspected of taking place in the home are under investigation (*Tessling* and *Patrick*). Where, as in the case at bar, there was no direct search of the home itself, the informational privacy interest should be the focal point of the analysis. The fact that information about the home was being sought requires that the informational privacy analysis be alive to the heightened privacy interest that the law recognizes for our homes. However, although informational and territorial privacy interests concerning the home may overlap in certain situations, this Court held under similar circumstances in *Tessling* that the fact that a home was involved "is an important factor but it is not controlling and must be looked at in context and in particular ... in relation to the nature and quality of the information made accessible" by the alleged search (para. 45).

96 This case is only incidentally a case of territorial privacy. The activities which the police observed on the Gnutella Network, and which they were investigating, led them to inquire about the particular IP connection which was involved in the uploading of suspected pornographic images. That connection turned out to be at a home. The home of Mr. Trapp was not directly searched or intruded on by virtue of the police inquiry of SaskTel. While it may be that a search and seizure of one's personal computer in one's home is an intrusive and extensive invasion of one's

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

privacy, in this case the request of SaskTel and the information received by the police by itself gave no access to the contents of Mr. Trapp's computer. The actual intrusion into Mr. Trapp's home and computer was accomplished by subsequent warrant, and not directly by the impugned conduct of the police, *i.e.* making the inquiry with SaskTel.

97 This case therefore primarily involves informational privacy, *i.e.* the right of an individual to keep his name and address private. In *Tessling*, *supra*, Binnie J., writing for a unanimous court, described informational privacy as a claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. He acknowledged that the reasonableness line is difficult to draw with respect to privacy generally and informational privacy particularly (para. 29).

98 In *Gomboc*, Deschamps J. in respect of informational privacy stated at paras. 27 and 28:

[27] The *Charter* guarantee of informational privacy protects the right to prevent certain personal information from falling into the hands of the state. The scope of constitutional protection will vary depending upon the nature of the information and the purpose for which it is made available (*R. v. Colarusso*, [1994] 1 S.C.R. 20, at p. 53; *Patrick*, para. 38).

[28] In *Plant*, Sopinka J. rejected a categorical approach to informational privacy, protecting only information that is "personal and confidential" (p. 293). He framed the constitutional protection given to informational privacy in the following purposive terms:

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. [p. 293]

Sopinka J. also outlined factors that could form the basis for a reasonable expectation of privacy which included: "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" (p. 293).

However not all information which fails to meet the biographical core test is open to the police. Binnie J. in *R. v. M. (A.)*, 2008 SCC 19, [2008] 1 S.C.R. 569 (S.C.C.), states at para. 68:

68 In *Dyment*, *Plant* and *Tessling*, the various categories of "information" (including "biographical core of personal information") were used as a useful analytical tool, not a classification intended to be conclusive of the analysis of information privacy. Not all information that fails to meet the "biographical core of personal information" test is thereby open to the police. Wiretaps target electrical signals that emanate from a home; yet it has been held that such communications are private whether or not they disclose core "biographical" information: *R. v. Duarte*, [1990] 1 S.C.R. 30; *R. v. Wiggins*, [1990] 1 S.C.R. 62, and *R. v. Thompson*, [1990] 2 S.C.R. 1111. The privacy of such communications is accepted because they are reasonably intended by their maker to be private: R. M. Pomerance, "Shedding Light on the Nature of Heat: Defining Privacy in the Wake of *R. v. Tessling*" (2005), 23 C.R. (6th) 229, at pp. 234-35.

99 Also in *Gomboc*, Deschamps J. at paras. 30 and 31 states the following:

30 As in *Plant*, the nature and quality of the information disclosed by the DRA and the absence of an expectation of confidentiality in respect of Enmax's customer information form part of the totality of the circumstances informing the reasonableness of the privacy expectation in the present case. I will examine the impact of each, starting with the absence of a confidentiality expectation.

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

31 The terms governing the relationship between Enmax and its customers are highly significant. Mr. Gomboc's expectation of privacy is informed by the *Code of Conduct Regulation* enacted pursuant to the *Electric Utilities Act*, S.A. 2003, c. E-5.1. The regulations permit disclosure of customer information "to a peace officer for the purpose of investigating an offence if the disclosure is not contrary to the express request of the customer" (s. 10(3)(f)). Mr. Gomboc did not request that his customer information be kept confidential. The *Code of Conduct Regulation* dovetails with s. 487.014 of the *Criminal Code*, which confirms that a peace officer may ask a person to voluntarily provide information that the person is not otherwise prohibited by law from disclosing. Their combined effect establishes that not only was there no statutory barrier to Enmax's voluntary cooperation with the police request, but express notice that such cooperation might occur existed.

100 In *R. v. Patrick*, 2009 SCC 17, [2009] 1 S.C.R. 579 (S.C.C.), Binnie J., writing for the majority, restates the totality of the circumstances analysis and outlines the following considerations going into whether or not there was an expectation of privacy in information: (1) the nature or subject matter of the alleged search; (2) the claimant's direct interest in the subject matter; (3) the claimant's subjective expectation of privacy in information contained in the subject matter and (4) the objective reasonableness of the expectation. With respect to the fourth factor, Binnie J. identified a number of sub-factors including (a) the place where the alleged search occurred; (b) whether the informational content of the subject matter was in public view; (c) whether such information was already in the hands of a third party; (d) whether the police technique was intrusive in relation to the privacy interest; (e) whether the evidence-gathering technique itself was objectively reasonable; and (f) whether the informational content exposed intimate details of the claimant's lifestyle or information of a biographic nature.

### ***C. Germane Internet Related Jurisprudence***

101 The case law respecting cases with similar or closely similar issues is thus far restricted to Provincial Court or Superior Court levels except for two cases which will be discussed *infra*. Mr. Trapp's counsel proffered a number of cases which determined that there was an expectation of privacy respecting use of the internet. Two of these, *R. v. Weir*, *supra* and the American case, *United States v. Maxwell*, *supra* dealt with privacy rights in connection with E-mail accounts, the last mentioned one dealing with warrantless access to extensive E-mail communications. Neither case is of assistance in this case, because the subject matter in this case concerns the privacy rights in respect of the internet activities of Mr. Trapp on a file-sharing network. Privacy rights in E-mail accounts are not at issue in this case.

102 Two other cases cited by Mr. Trapp, *R. v. Kwok*, *supra* and *R. v. Cuttell*, *supra*, concerned facts similar to the facts of this case. In *Kwok*, the accused had traded pornographic images with an undercover officer on the internet and was subsequently charged with possessing and distributing child pornography. The police thereafter learned of Kwok's identity by requesting and receiving subscriber information from Rogers Cable under the authority of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 ("*PIPEDA*") which, as in this case, was incorporated into a warrant to search Kwok's residence. The court determined that Kwok's s. 8 *Charter* rights and personal expectation of privacy had been breached because personal information such as names and addresses of customers held by companies such as Rogers Cable would tend to disclose the intimate details of lifestyle choices. The court excluded the evidence obtained pursuant to the warrant. *Kwok*, however, did not address the issue of the contractual agreement between Rogers and Kwok.

103 In *Cuttell*, the police located an IP address they believed was sharing images of child pornography on the internet and subsequently requested the subscriber's name and address for that IP address from Bell Canada without first seeking a warrant. In arriving at the conclusion that Cuttell had a reasonable expectation of privacy in his subscriber information and that s. 8 had been breached, the court relied on *Kwok*. The court also found that there was no specific evidence before it respecting Cuttell's contractual obligations with Bell or even any general evidence of Bell's usual practice in relation to customer obligations. In the end, the court determined that despite the s. 8 breach, the evidence would be admitted.

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

104 In light of *Gomboc*, the commercial relationship between the subscriber and the company providing information is a significant factor, given the contextual approach to determination of a reasonable expectation of privacy. In my view, both *Kwok* and *Cuttell* are distinguishable because of the absence of any evidence respecting the contract and how it affected the expectation of privacy.

105 In *R. v. Chehil*, 2009 NSCA 111, 248 C.C.C. (3d) 370 (N.S. C.A.), the court was dealing with ticketing information including name and baggage details disclosed by WestJet to the police as part of a police program to curtail drug trafficking. The court observed that WestJet was not obligated to keep the ticketing and baggage information confidential because it was by the general terms of the ticketing agreement allowed to disclose it to government agencies and also because *PIPEDA* authorized disclosure for law enforcement purposes. After doing a totality of circumstances analysis, the court concluded that there was no reasonable expectation of privacy and that a search within the meaning of s. 8 of the *Charter* had not occurred.

106 In *R. v. Ballendine*, 2011 BCCA 221, 271 C.C.C. (3d) 418 (B.C. C.A.), the court dealt with child pornography related charges and the validity of a search warrant. Information in the warrant had been provided by the accused's ISP. In this case, however, the court determined that it did not have enough evidence of the terms of the ISP contract with the accused for that issue to be determined and the case was decided without that issue being dealt with.

107 In *R. v. Vasic* (2009), 185 C.R.R. (2d) 286 (Ont. S.C.J.), an Ontario case similar to this one, the court, citing *Kwok*, determined that disclosure of the name and municipal address of the holder of the IP address provided details of the lifestyle and personal choices of the individual, but because, pursuant to the agreement with Vasic, there was no obligation on Rogers (the ISP) to keep that information confidential, Vasic had no reasonable expectation of privacy and there was no breach of Vasic's s. 8 *Charter* rights.

108 In *R. v. Ewanyshyn*, unreported, March 29, 2009 (Alta. Q.B.), again a case similar to this one, the court determined that the commercial relationship between the ISP and the accused was not confidential respecting the name, address and phone number of the accused. The Court also found that this information obtained from the ISP provided little biographical core information or insight into his private life. The Court determined that he had no reasonable expectation of privacy in that information and that s. 8 was not breached.

109 In *R. v. Brousseau*, 2010 ONSC 6753, 264 C.C.C. (3d) 562 (Ont. S.C.J.), also a case similar to this one, the court found that the Terms of Service documents disclaimed any confidentiality or privacy with respect to information held by Rogers, the ISP. The court determined the subscriber information on its own did not reveal any core biographical information and said very little about the intimate details of the lifestyle and personal choices of the individual. The court found that the accused had no reasonable expectation of privacy in his name and address as provided to the police by Rogers. The court at paras. 47-49 stated as follows:

47 In sum, on the totality of the circumstances, I find the Applicant had no reasonable expectation of privacy in the information, that is, his name and address, provided by Rogers to the police.

48 Rather, the Applicant of his own accord used a file sharing system that enabled the police to look at the files on his computer. The provisions in the Rogers documents repudiate the suggestion of confidentiality in these circumstances, given that Rogers specifically indicates, among other things, that it can disclose information to comply with legal process and to ensure compliance with its user agreement. These factors in my view distinguish this case from *Kwok*; however, in any event, I respectfully disagree with the conclusion in *Kwok*. The information at issue, that is, the Applicant's name and address, is general information routinely exchanged as part of commercial interactions. It does not affect his dignity, integrity or autonomy, nor does it reveal that biographical core of personal information to which the cases refer. The request was made under the authority of *PIPEDA*, and responded to by Rogers in accordance with its own administrative policies.



2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

49 Accordingly, all of these factors lead me to find that there has been no breach of the Applicant's section 8 right.

110 In *R. v. McNeice*, 2010 BCSC 1544 (B.C. S.C.), again a similar case to this one, the court determined that internet subscriber information limited to name and address was not biographical information that one could reasonably expect to be kept private from the state. Citing *R. v. Wilson*, [2009] O.J. No. 1067 (Ont. S.C.J.), the Court said at para. 49:

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.

As is evident a great number of the trial level decisions take the approach that internet subscriber information limited to name and address is not core biographical information one could reasonably expect to keep from the state.

111 The result in the foregoing cases accords with the American approach to internet subscriber information. A number of cases in the United States including *United States v. Perrine*, 518 F.3d 1196 (U.S. C.A. 10th Cir. 2008), 1204-1205, *United States v. Bynum*, 604 F.3d 161 (U.S. C.A. 4th Cir. 2010), 164-165, and *United States v. Stults*, 575 F.3d 834 (U.S. C.A. 8th Cir. 2009) have concluded that subscriber information given to an internet provider is not protected by the Fourth Amendment's privacy expectations.

112 The cases also suggest that the presence or absence of legislation which speaks to the issue of privacy of information and exceptions thereto is a relevant component of the contextual analysis in a s. 8 determination such as this.

113 In *Ewanyshyn*, *supra*, the Crown argued that *PIPEDA* merely allowed the ISP Shaw to choose whether it would comply with a police request and that therefore there was no search and s. 8 was not engaged. The Court proceeded on the assumption without deciding the issue that the *PIPEDA* request was for a search and held that the search was reasonable on the facts of that case.

114 In *R. v. Ward*, 2008 ONCJ 355, 176 C.R.R. (2d) 90 (Ont. C.J.), Lalande J. held that *PIPEDA* is permissive and

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

does not create a new search power or defeat a person's *Charter* protection against unreasonable search and seizure. In *Wilson, supra*, Leitch J. at para. 39 states:

39 PIPEDA does not compel the disclosure of information. That legislation simply permits an internet service provider to disclose information and it may in fact decline to produce information requested by a law enforcement agency.

115 In *Brousseau, supra*, Croll J. respecting *PIPEDA* states as follows at paras. 41-45:

41 It cannot be in dispute that the police must investigate crime; that is their duty: see *Hill v Hamilton-Wentworth Regional Police Services Board*, 2007 SCC 41, [2007] 3 S.C.R. 129 at para. 55. In my view, when D/C Purchas sent the Letter of Request for Account Information Pursuant to a Child Exploitation Investigation to Rogers, he was acting in the lawful execution of his duties to investigate crime, prevent crime and apprehend criminals.

42 PIPEDA grants authority to an organization to use and disclose information that it has collected for the purpose of assisting with an investigation of the contravention of the laws of Canada. There is no requirement for a court order. Upon receipt of this request, Rogers could have refused to provide the information. ...

43 It is also not in dispute that the enactment of PIPEDA was focused on protecting the privacy rights of Canadians. However, I do not read the legislation as requiring that the police obtain judicial pre-authorization prior to information being disclosed when the organization, such as an ISP like Rogers, has the lawful authority to disclose as long as it has reasons to believe there is an investigation relating to the enforcement of a law of Canada.

...

45 The Applicant submits that the overriding policy consideration behind PIPEDA is the privacy of personal information and that its terms do not confer lawful authority on the police to conduct a warrantless search. With respect, I do not consider the request for information to be a warrantless search. Section 7 of PIPEDA is a permissive provision that allows an organization to provide the requested information. The organization, as well, could refuse to provide the information. In this case, as part of their investigation, the police simply asked for information from a third party that is not bound by an obligation of confidentiality to the Applicant. In my view, this is something that the police must routinely be allowed to do as part of their job. (See also the conclusions in *Wilson, supra*, at para. 38.)

116 In *McNeice, supra*, the Court at para. 43 in relation to s. 487.014(1) of the *Criminal Code* and *PIPEDA* stated the following:

43 It seems clear to me that, absent a finding of state agency, s. 487.014(1) provides the police with lawful authority to make a PIPEDA request for subscriber information, which an ISP is not prohibited by law from disclosing if it falls within the provisions of s. 7(3)(c. 1)(ii) of PIPEDA, which reads as follows:

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

117 These cases affirm that the privacy legislation authorizes disclosure by the holder of the information in certain circumstances but does not in itself empower the police.

118 With this jurisprudence in mind, we turn to the *Patrick* analysis of whether on the totality of these circum-



2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

stances, Mr. Trapp had a reasonable expectation of privacy in the Information.

#### ***D. Application of the Totality of the Circumstances Analysis***

##### ***(i) Subject Matter***

119 The relevant subject matter of the alleged search was Mr. Trapp's name, an address and a telephone number. Implicit in that information is that at the relevant time, SaskTel was providing internet service to Mr. Trapp of that address and that he was being billed for that service. This information in itself does not identify the person operating the computer attached to the internet connection at the relevant time. For example, it may be that others have access to and use the internet connection, in which case further investigation by the police would be necessary. However, the Information furthered the investigation and ended up linking the activity, observed by the police on the peer-to-peer network, to Mr. Trapp. Some of the information which Shepherd received, such as Mr. Trapp's e-mail address, his cell phone number, and his subscription to Max cable, went beyond what the police sought. The police had no need of this additional information given their investigation to that point.

##### ***(ii) Claimant's Interest in Subject Matter***

120 The Crown does not dispute that Mr. Trapp would have an interest in the subject matter.

##### ***(iii) Subjective Expectation of Privacy***

121 The next question is whether Mr. Trapp had or is presumed to have had a subjective expectation of privacy in the informational content respecting his subscriber information. In this case, Mr. Trapp did not testify. However, as in *Patrick, supra*, the absence of direct evidence from an accused about his subjective expectation of privacy does not end the matter. In *Ewanyshyn, supra*, the court held that even though the accused failed to testify, the court was prepared to infer that he had a direct interest in his name, address, and phone number being provided to the police and thus had a subjective expectation of privacy. The Crown argues that there is no subjective expectation of privacy in this case because the information revealed nothing about activities taking place in the home and because information of this type was widely available and distributed through telephone and other public directories. In most cases, the average user of the internet would have an expectation that information related to their internet use, including the fact they are internet users, would be kept confidential except to those to whom they wish to disclose the information. For the purposes of this analysis, I am prepared to assume that there is a subjective expectation of privacy.

##### ***(iv) Objective Reasonableness of Expectation of Privacy***

122 Whether an objective reasonable expectation of privacy exists can be analyzed in the context of the factors as outlined by Sopinka J. in *Plant, supra* and Binnie J. in *Patrick, supra* as mentioned earlier and the other relevant factors identified in the jurisprudence.

##### **(a) Place of Search**

123 In this case, the search occurred at the offices of SaskTel, which was a place where Mr. Trapp had no reasonable expectation of privacy whatsoever.

##### **(b) Was Information Public**

124 Although Mr. Trapp's E-mail addresses and IP address were not public, the name and part of the account information of Mr. Trapp provided by SaskTel was available to the public in the Saskatoon phone book. This militates

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

against a reasonable expectation of privacy.

**(c) Was Information in Hands of Third Party**

125 Mr. Trapp's account information was also in the hands of SaskTel, a third party. This factor is neutral because the basis on which SaskTel held the information is important.

**(d) Contractual Expectations of Confidentiality**

126 Another part of the context is the expectation of confidentiality between SaskTel and Mr. Trapp and the terms on which SaskTel held the information. The relationship between SaskTel and Mr. Trapp is a commercial one which is governed by numerous terms and conditions in the Terms of Service. Articles 69.1 and 69.4 state that all customer information SaskTel has is confidential. However, there is an exception for the name, address and phone number where it is published in the directory or available through directory assistance. Article 69.2 allows a customer to request that their name, address and phone number not be published or available on directory assistance in which case it would, by virtue of Article 69.1, be confidential. Article 57.1 of the Terms of Service makes it clear that the services are not to be used for any illegal purpose nor in an illegal manner.

127 Article 69.4 reads that unless a customer provides express consent, the information of a customer "other than the customer's name, address and listed telephone number is confidential and may not be disclosed by SaskTel to anyone other than" certain specific persons under specific circumstances. Interestingly SaskTel appears by virtue of Article 69.4(f) to be able to disclose even confidential information to an agent of a public authority "if in the reasonable judgment of SaskTel it appears that there is an imminent danger to life or property which could be avoided or minimized by disclosure of the information". Article 69.5(c) states that despite the restrictions in 69.4 SaskTel may disclose confidential customer information if

(c) SaskTel is otherwise legally empowered to disclose the information.

128 For the purposes of this analysis it is clear that as between SaskTel and Mr. Trapp, the general rule is that customer information is confidential, but the contractual expectation is that his name, address and telephone number are not confidential. In this case, there is no evidence that Mr. Trapp's name, address and phone number were not to be published. Mr. Trapp also was in breach of the Terms of Service by using the services for an illegal purpose or manner. Even if the information were confidential, SaskTel may, pursuant to Articles 69.4(f) and 69.5(c) disclose this information to a public authority and also disclose it where it is otherwise legally empowered to do so. *A fortiori* SaskTel is not contractually bound to refuse to disclose to the police information which is in this case not confidential. The lack of contractual confidentiality militates against a reasonable expectation of privacy.

**(e) Relevant Statutory Provisions**

129 With respect to statutory legal empowerment to disclose, section 29(2)(g) of *FIPPA* permits SaskTel to release information which is requested in relation to a criminal investigation. It reads as follows:

(2) Subject to any other Act or regulation, personal information in the possession or under the control of a government institution may be disclosed: ....

(g) to a prescribed law enforcement agency or a prescribed investigative body:

(i) on the request of the law enforcement agency or investigative body;

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

(ii) for the purpose of enforcing a law of Canada or a province or territory or carrying out a lawful investigation; and

(iii) if any prescribed requirements are met; ....

This provision is similar to one in *PIPEDA*. The comments of Croll J. in *Brousseau, supra* in respect of *PIPEDA* are also apt in the case of s. 29(2)(g) of *FIPPA*. This section is an authorization for the disclosing agency if it wishes to do so, rather than an empowerment for the police to gather the information. But in my view it is another basis or justification for SaskTel to make disclosure of personal information in the proper case, especially in the presence of contractual permission in Article 69.5(c).

130 Generally, the police have the authority and power to investigate crime as observed by Croll J. in *Brousseau, supra*. In this case, Shepherd was acting in the lawful execution of her duty to investigate an apparent crime when she sent the request to SaskTel. Section 487.014 of the *Code* is therefore germane. It reads as follows:

#### **Power of peace officer**

**487.014 (1)** For greater certainty, no production order is necessary for a peace officer or public officer enforcing or administering this or any other Act of Parliament to ask a person to voluntarily provide to the officer documents, data or information that the person is not prohibited by law from disclosing.

This provision confirms that a peace officer may ask a person to voluntarily provide information that the person is not otherwise prohibited by law from disclosing. Deschamps J. cites this section of the *Code*, in *Gomboc* at para. 31, as a factor in the analysis which read together with any other relevant statute can establish that not only is there no statutory barrier to co-operation with a police request, but express notice that such co-operation might occur. Because of the applicability of s. 29(2)(g) of *FIPPA*, SaskTel, in this case, was not prohibited by law, from disclosing the Information, and this factor, along with the absence of any contractual impediment, and indeed a contractual non-confidentiality clause respecting name, address and telephone number, weighs against a reasonable expectation of privacy.

#### **(f) Intrusiveness**

131 Sopinka J.'s comments in *Plant* at p. 295, are apt respecting the next element, the intrusiveness of the investigative technique:

The place and manner in which the information in the case at bar was retrieved also point toward the conclusion that the appellant held no reasonable expectation of privacy with respect to the computerized electricity records. The police were able to obtain the information on-line by agreement of the Commission. Accessing the information did not involve intrusion into places ordinarily considered private... Nor did it involve invasion by state agents in personal computer records confidentially maintained by a private citizen.

The letter requesting information was not intrusive. It involved no interference with Mr. Trapp's personal or bodily integrity. It involved no direct access to the house where the internet connection was located and by itself provided no particulars of what was going on in the house or the content of the use of the computer at the relevant time. It also provided no information about whether Mr. Trapp was operating the computer at the relevant time. The intrusion into privacy under these circumstances was a minimal and proportional way of determining who the anonymous user of the specific IP address was. The lack of intrusiveness militates against a reasonable expectation of privacy.

#### **(g) Reasonableness of Evidence-Gathering Technique**

2011 CarswellSask 785, 2011 SKCA 143, 377 Sask. R. 246, 528 W.A.C. 246, [2012] 4 W.W.R. 648

132 The standard for assessing whether the evidence-gathering technique is reasonable is whether it undermines privacy and has the "potential to make social life in this country intolerable" (*Patrick* at para 70). The Saskatoon Police Service did not gain unlimited and continuous access to information in SaskTel's database. The letter was specific as to IP address and the subscriber of the address at a specific point in time. With the advent of crimes involving the internet, the letter was a reasonable way for police to determine the identity of someone allegedly committing prohibited acts using a file-sharing network on the internet. The technique employed by the police in this case was objectively reasonable.

#### **(h) Is the Information of an Intimate, Biographical or Otherwise Private Nature**

133 On the matter of whether a particular kind of information is protected, Deschamps J. in *Gomboc* formulated the question as follows:

34 ... Rather, the appropriate question is whether the information is the sort that society accepts should remain out of the state's hands because of what it reveals about the person involved, the reasons why it was collected, and the circumstances in which it was intended to be used.

134 The name and address, or for that matter telephone number alone, in this case provide no further insight into Mr. Trapp's private life apart from what Mr. Trapp already exposed by his participation in the peer-to-peer network. Disclosure of this information in this case does not affect his dignity, integrity or autonomy any more than it is already affected by his sharing of images on his computer with other internet users. In a case such as this, where Mr. Trapp has put into the public realm, on the Gnutella network, information about his activities or lifestyle, and it has come to the attention of the police, the state is entitled to investigate the identity of whom it is dealing with since he has come to the attention of the state by lawful means. In the circumstances, the information was collected for a legitimate purpose, *i.e.* the furtherance of the child pornography investigation.

135 The totality of the foregoing *Patrick* factors all weigh against an objective expectation of privacy by Mr. Trapp in his name, address and phone number respecting his IP address in this case. These factors include the absence of any disclosure of any further core biographical information or intimate details about Mr. Trapp or his life (apart from what he displayed on the Gnutella Network), SaskTel's contractual right to disclose the information, the availability of this information to the public, the lack of any legal barrier to its disclosure and the facilitation of its disclosure by both *FIPPA* and the *Criminal Code*, the minimal intrusiveness of the request, and the reasonableness of the technique employed. This result accords generally with the weight of the cases mentioned earlier.

#### **V. Conclusion**

136 On the totality of circumstances, there is no reasonable expectation of privacy in Mr. Trapp's name, address and phone number respecting his IP address in this case. The trial judge made no error in finding there is no search and seizure and violation of s. 8 of the *Charter*. The appeal is accordingly dismissed.

*Appeal dismissed.*

FN1 In fact SaskTel imprudently provided the police with more information than this, including information about which television channels the accused had subscribed for, but for present purposes that is neither here nor there.

END OF DOCUMENT

**VOLTAGE PICTURES LLC**  
Plaintiff

and

Court File No. T-2058-12  
**JOHN DOE and JANE DOE**  
Defendants

**FEDERAL COURT**

Proceeding commenced at Toronto

**MOTION RECORD OF THE PLAINTIFF,  
VOLTAGE PICTURES LLC**  
*(Motion for a written examination of a non-party,  
returnable December 17, 2012)*

**BRAUTI THORNING ZIBARRAS LLP**  
151 Yonge Street, Suite 1800  
Toronto, ON M5C 2W7

**James Zibarras**  
LSUC No. 48856F

**John Philpott**  
LSUC No. 60246U

Tel.: 416.362.4567  
Fax: 416.362.8410

Lawyers for the Plaintiff,  
**VOLTAGE PICTURES LLC**