ONTARIO BAR ASSOCIATION
A Branch of the Canadian Bar Association

CRIMINAL JUSTICE

Volume 22, No. 1 – September 2012 Criminal Justice Section

Digital Evidence meets the Charter: Peer-to-Peer (P2P) File-Sharing Networks

A case comment on *R. v. Spencer* and *R. v. Trapp*

Brock Jones[1]

A. Peer-to-Peer File Sharing Networks

Peer-to-peer (P2P) file sharing networks allow users to share files with one another over the internet without the need for a central depository. While these technologies have undoubtedly helped facilitate the free exchange of information and other lawful materials, they have also accelerated both the proliferation of and access to online child pornography. In response, police investigative techniques designed to thwart such activities have had to rapidly evolve to keep pace.

In the recent decisions of *R. v. Trapp*[2] and *R. v. Spencer*[3], the Saskatchewan Court of Appeal had occasion to address two such cases involving P2P file sharing networks. Both offenders had accessed such networks and downloaded child pornography. In both cases the police obtained personal subscriber information about the offenders from their respective internet service providers (ISPs) without a warrant. Spencer and Trapp challenged the lawfulness of this aspect of the police investigations, claiming their rights under section 8 of the *Charter* had been infringed.

Two different panels of the Court released a total of five separate decisions in deciding the cases, demonstrating the difficulty in finding consensus in this complex and emerging area of the law. But while the justices' methods of analysis differed in significant regards, the results were unanimous: both offenders' *Charter* applications were dismissed and their convictions upheld.

As the leading criminal law appellate level decisions in Canada on this subject matter, understanding the nature of the debate between the various judgments at play in these twin cases is absolutely essential. In addition to providing important holdings on the nature of privacy rights in supposedly anonymous online activity, the Court makes some interesting observations about the intersection of

---

[1] Brock Jones, Assistant Crown Attorney, Ministry of the Attorney General; Adjunct Professor, Faculty of Law, University of Toronto. The views expressed herein are personal to the author and do not represent those of the Attorney-General of Ontario or the Crown Attorney's Office.
[2] 2011 SKCA 143.
[3] 2011 SKCA 144.

the *Criminal Code* and the *Personal Information and Protection and Electronic Documents Act ("PIPEDA")*[4].

I. Background Facts and Police Investigations

Both *Spencer* and *Trapp* involved police investigations into illicit activity taking place via two P2P file sharing networks – LimeWire[5] and Gnutella.

In *Trapp*, a police officer was monitoring the Gnutella P2P file sharing network on the internet. She accessed Trapp's "shared files" and located child pornography. Trapp's internet protocol (IP) address was freely broadcast over the network. The officer generated an "IP history" for Spencer's computer and determined the ISP granting him access was SaskTel.

The officer then sent a "letter of request" to SaskTel for personal information about the IP address in question. SaskTel confirmed the IP address belonged to Trapp. Officers executed a search warrant at his residence that included his personal computer where they located child pornography files.

In *Spencer*, the offender obtained a number of files containing child pornography over the internet through the file-sharing program LimeWire. He retained the files in a shared folder on his personal computer and others were able to view and download the child pornography.

An officer with the Saskatoon Police Service logged onto the LimeWire network and located the child pornography in the shared folder. The IP address associated with the computer hosting the shared folder was publicly available.

The officer then sent a "letter of request" for the "customer identifying information" surrounding that subscription account to Shaw Communications (the ISP.) Shaw Communications is a privately incorporated organization, similar to Bell or Rogers.

Shaw complied and a warrant was obtained to search the residence in question. Spencer's computer was seized and searched and child pornography was located on its hard-drive.

II. Were Spencer and Trapp's Reasonable Expectations of Privacy violated?

The majority of the Court in *Trapp* held that the offender did maintain a reasonable expectation of privacy in his subscriber information held by the ISP, notwithstanding his access and use of a file sharing network. As stated by the Court, "[w]hen one subscribes for Internet access service, one does not surrender one's expectation of privacy regarding what one chooses to access on the Internet."[6]

---

[4] S.C. 2000, c.5.

[5] It is worth nothing that LimeWire effectively closed its operations in October 2010 following a US federal judge's finding that it was liable for copyright infringement and issued a permanent injunction to shut down its operations [see: *Arista Records et al. v. Lime Group* 715 F. Supp. 2d 481 (2010)]. Nevertheless, various P2P networks remain active and alive with users, such as Frostwire, BitTorrent and many others.

[6] See para [39].

However, the majority also held that the "search" in question was a reasonable one and thus no violation of section 8 of the *Charter* occurred. The latter conclusion was derived primarily from a combination of section 487.014(1) of the *Criminal Code* and section 29 of Saskatchewan's *The Freedom of Information and Protection of Privacy Act.* The combination of these two Acts justified the police "letter of request" for SaskTel to provide subscriber information, and SaskTel's decision to provide that information voluntarily.

As such, the search was authorized by law, the law was reasonable and the manner in which the search was conducted was reasonable.

Unlike the majority in *Trapp,* in *Spencer,* two judges – Caldwell J.A. and Ottenbreit J.A. – held the accused had no reasonable expectation of privacy in the internet subscriber information in question. While agreeing with the analytical structure adopted by Cameron J.A. in *Trapp*, the majority found the contractual agreement with Shaw Communications, which explicitly contemplated disclosure to the authorities upon request, to be a strong factor detracting from *Spencer's* claim he had a *reasonable* expectation of privacy in his subscriber information.

Furthermore, the combination of section 487.014(1) of the *Code* and section 7(3) of ``*PIPEDA*`` - which applies to private businesses - allowed for the police letter of request in question. Section 7(3)(c.1) of *PIPEDA* in particular authorized the voluntary disclosure of "an individual's personal information to the police by a third party without the individual's knowledge or consent", if the disclosure was "made to a government institution […] for the purpose of administering any law of Canada."

This factor also militated against finding a reasonable expectation of privacy in the subscriber information.

III. Understanding The Intersection of Section 487.014 of the *Criminal Code* and Section 7 of *PIPEDA*

At the heart of the decisions in *Spencer* and *Trapp* is the premise contending that even if one can characterize the police requests for personal information about the offenders' subscriber information as "searches" under section 8 of the *Charter*, they were nevertheless reasonable as they were authorized by a combination of section 487.014 of the *Code* and section 7 of *PIPEDA* (or the applicable provincial statute, should one exist). A more thorough understanding of *PIPEDA* in particular is thus crucial to understanding the implication of these rulings, as these letters are becoming increasingly common in police investigations into crimes of internet child exploitation.

PIPEDA places restrictions on how private sector organizations may collect, use or disclose personal information in the course of commercial activities.

In *Spencer* the police sent a "letter of request" to the ISP in question seeking the release of private information surrounding unknown subscribers. This is a commonly utilized device for officers investigating crimes of internet child exploitation. The letter was authorized, and lawful, the Court held, based on an intersection between section 487.014 of the *Criminal Code* and section 7 of *PIPEDA.*

A closer examination of these sections is required to fully grasp the extent of this holding in *Spencer*.

Section 487.014(1) of the *Criminal Code* 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

Section 7(3) of *PIPEDA* permits the disclosure of an individual's personal information to the police by a third party without the individual's knowledge or consent 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
>
> (i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,
>
> (ii) the disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or
>
> (iii) the disclosure is requested for the purpose of administering any law of Canada or a province;

Section 487.014 of the *Code* therefore effectively 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. As section 7 of *PIPEDA* authorizes requests for disclosure, the combination of these sections potentially opens up vast realms of personal information held by third party corporations to the police without requiring a formal court order authorizing its release.

If the reasoning in *Spencer* is adopted by the courts in other provinces, the only means for the defence to successfully challenge the legality of these "letters of request" will be to attempt to demonstrate that the private entity in question (typically an ISP) was in fact acting as a state agent, thereby attracting *Charter* scrutiny.[7] In the absence of evidence to support such a finding, the Crown should successfully be able to have motions for *Charter* relief in this context dismissed on a simple jurisdictional basis.

B. Conclusions

Police investigations into child pornography offences are increasingly taking place in the domain of online file-sharing. Familiarity with the technologies themselves, including the particular nature of

[7] See *RBC v. Ren* 2009 ONCA 48

the file-sharing software in question and any wireless networks that form part of the investigation will be essential for counsel.

The legal landscape in this area is constantly shifting. It remains to be seen if the analysis in *Spencer* and *Trapp* is adopted by appellate courts in other provinces. Conflicting case law in Ontario at the trial level remains unsettled.[8] American jurisprudence is also largely in its infancy.

Furthermore *Spencer* and *Trapp* do not address what information, if any, the police must have at their disposal before sending a "letter of request." Is there any requirement they demonstrate to the ISP (or ultimately a court) that they had at least a reasonable suspicion the IP address in question was engaged in illicit online activity to afford themselves the protections of section 487.014(1) of the *Code*?[9] Or is the standard higher, requiring reasonable and probable grounds?[10] Or is there no standard whatsoever, and the police need not require any grounds whatsoever and may merely send the letters once they are simply engaged in any online investigation?[11]

Resolving this question will require further litigation. This paper presented a brief overview of the leading Canadian appellate decisions in this area as of the time of this article's publication. Further comments, feedback or insights are welcomed.

[8] See *R. v. Brousseau* 2010 ONSC 6753 cited favourably in *R v. Trapp*; *contra:* see *R. v. R.* v. *Kwok*, [2008] O.J. No. 2414 (QL); *R.* v. *Cuttell*, 2009 ONCJ 471 (CanLII), 2009 ONCJ 471, 247 C.C.C. (3d) 424.

[9] See *R. v. Mann* [2004] 3 S.C.R. 59 for the requirements the authorities requirement to begin a lawful investigative detention, perhaps a rough analogy to the online investigations in *Spencer* and *Trapp*.

[10] It is worth nothing that section 487.012 of the *Code*, enabling production orders, and passed by Parliament in the same set of legislative amendments that included section 487.014 of the *Code*, sets a requirement of "reasonable grounds" in an *ex parte* hearing.

[11] For example, in *R. v. Suberu* 2009 SCC 33, the Supreme Court affirmed that not all police questioning triggers a detention, and thus one's *Charter* rights.