TOP FIVE 2014

Each year at OJEN's Toronto Summer Law Institute, a judge from the Court of Appeal for Ontario identifies five cases that are of significance in the educational setting. This summary, based on these comments and observations, is appropriate for discussion and debate in the classroom setting.

R. v SPENCER, 2014 SCC 43.

Date Released: June 13, 2014

https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/14233/index.do

Facts

18 year-old Matthew David Spencer, of Saskatoon, used LimeWire, which is a free peer-to-peer file-sharing program, to download and store child pornography. He was living with his sister at the time and was using internet service registered to her name. Peer-to-peer systems such as LimeWire do not have one central database of files, but instead allow their users to share files with other users. Such systems are commonly used to download music and movies.

A Saskatoon police officer signed onto LimeWire to search for users sharing child pornography. When Spencer's computer was connected to LimeWire, the officer was able to browse the contents of his "shared folder", which was available to all LimeWire users. The officer saw what he believed to be child pornography in the folder. Through further investigation, police were able to determine the Internet Protocol (IP) address of Spencer's computer, that was in Saskatoon and that Shaw Communications Inc. (Shaw) was the Internet Service Provider (ISP).

The police made a "law enforcement request" to Shaw for the subscriber information including the name, address and telephone number of the customer using that IP address. The request was made under s. 7(3)(c.1)(ii) of the *Personal Information Protection and Electronic Documents Act (PIPEDA)*.

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

7(3). […]an organization may disclose personal information without the knowledge or consent of the individual only 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 related to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law.

The request indicated that police were investigating child pornography and that the subscriber information was being sought as part of an ongoing investigation. The police did not have, nor did they try to obtain, a search warrant. Shaw complied with the request and provided Mr. Spencer's sister's personal subscriber information. As a result, Mr. Spencer was identified and charged with possessing and making available child pornography, which are offenses under the *Criminal Code of Canada*.

Canadian Charter of Rights and Freedoms

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

24(1). Anyone whose rights or freedoms, as guaranteed by this *Charter*, have been infringed or denied may apply to a court of competent jurisdiction to obtain such remedy as the court considers appropriate and just in the circumstances.

(2). Where, in proceedings under subsection (1), a court concludes that evidence was obtained in a manner that infringed or denied any rights or freedoms guaranteed by this *Charter*, the evidence shall be excluded if it is established that, having regard to all the circumstances, the admission of it in the proceedings would bring the administration of justice into disrepute.

Procedural History

At trial, Spencer was convicted of possession of child pornography but acquitted of making available child pornography. The Saskatchewan Court of Appeal affirmed the conviction for possession, set aside the acquittal for making available child pornography and ordered a new trial. Mr. Spencer appealed both the conviction and the new trial order to the Supreme Court of Canada (SCC).

Issues

1. Did the conduct of the police in obtaining the subscriber information from the ISP constitute a "search" within the meaning of s. 8 of the *Charter*?
2. If so, was the search authorized by law?
3. If not, should the evidence obtained as a result be excluded pursuant to s. 24(2) of the *Charter*?

Decision

The SCC unanimously dismissed the appeal. Justice Cromwell, writing for the Court, found that the request by the police for the subscriber information indeed constituted a "search" within the scope of s. 8 of the *Charter*. Furthermore, the search was not conducted legally. However, the SCC ultimately decided that the evidence obtained through the unauthorized search should not be excluded from the record in the new trial.

Ratio

Whether police conduct is considered a search or seizure for the purposes of s. 8 of the *Charter* depends on whether the accused had a reasonable expectation of privacy in the information produced. The Court found that there is a reasonable expectation of privacy in subscriber information like that produced by Shaw to the police. The disclosure of this information will often amount to the identification of a user and expose his or her intimate or sensitive activities being carried out online, usually on the understanding that these activities are anonymous. Accordingly, a request by a police officer to an ISP for the voluntarily disclose such information amounts to a search.

Reasons

At trial, Spencer argued the police had infringed his right to be secure against unreasonable search or seizure under s. 8 of the *Charter*. The SCC first had to determine whether the conduct of the police was indeed a search. In examining the connection between the police's investigative technique and the privacy interest at stake, the SCC not only looked at the nature of the precise information sought, but also at the nature of the information that it reveals. Writing for the SCC, Justice Cromwell took the view that the basic information regarding the identity of a subscriber of an internet connection (like their name and address) is linked to particular, monitored Internet activity and would reveal intimate details of the lifestyle and personal choices of the individual. This is important since an internet user only reveals this intimate personal information with the belief that their online activities are anonymous.

The SCC explored whether Mr. Spencer's expectation of privacy in this case was reasonable. It examined Shaw's Terms of Service since they were relevant in assessing the reasonableness of a subscriber's expectation of privacy. Shaw's Terms of Service, taken as a whole, provided a confusing and unclear picture of what it would do when faced with a police request for subscriber information. Since the Terms of Service could not be relied on to justify the disclosure of subscriber information, the SCC found that Spencer's expectation of privacy was indeed reasonable.

The next question examined by the SCC was whether s. 7(3)(c.1)(ii) of *PIPEDA* authorized the disclosure of personal information. That section of the law allows an organization to disclose personal information as long as the request is made by someone with the "lawful authority" to make it. For the police to have lawful authority, they would need either a warrant or a statute (law) authorizing them to act.

The SCC was not convinced that the police could properly identify its lawful authority to obtain the subscriber information in these circumstances without the support of a warrant. Other sections of *PIPEDA* specifically require telecom companies to disclose private information when the police do have a warrant. From this, the

SCC determined that *PIPEDA* was effectively creating an investigative power for police to get information that would normally require a warrant without seeking one. The Court noted that because the stated purpose of *PIPEDA* was actually to increase individual privacy, this was inconsistent with the intent of the legislation. *PIPEDA* could not serve as the authority to demand information – that would require new and duly enacted legislation for that explicit purpose. Without appropriate legal authority, the disclosure was an infringement of Mr. Spencer's privacy.

Justice Cromwell clarified that the illegality of Mr. Spencer's actions did not cancel his privacy rights. As Mr. Spencer was engaged in online activity for which he had a reasonable expectation of privacy and anonymity, the police had no authority to force Shaw to provide identifying information. Without a warrant, the police could **ask** for the information, but they had no authority to **compel** Shaw to grant the request. In other words, privacy rights mean the police cannot use anonymous IP addresses as the starting point in "fishing expeditions" to identify specific suspects for investigation. However, the SCC was clear that an ISP in general has a legitimate interest in preventing crimes committed through its services, thus entirely different considerations may apply where an ISP detects illegal activity on its own and wishes to report this activity to the police.

Section 24(2) of the *Charter* provides the courts with a test that can be used to determine whether evidence of a crime that was collected through a violation of *Charter* rights can still be presented at trial. Two key points in this test are a) whether the police were acting in good faith in their investigation, and b) whether public perception of the justice system would be harmed more by including or excluding the evidence. Although Mr. Spencer's constitutional right against unreasonable search was violated, the SCC found that the police were acting by what they reasonably thought were lawful means to pursue an important law enforcement purpose. In the Court's view, the nature of the police conduct in this case would not harm public perceptions of the justice system. On the contrary, the offences in this case were serious and society had a strong interest in prosecuting Mr. Spencer. Therefore, the SCC ruled that excluding the evidence would bring the administration of justice into disrepute. The lower court's conviction for possession of child pornography was upheld and a new trial was ordered for Mr. Spencer on the charge of making child pornography available.

DISCUSSION

1. How well do you understand your ISP's privacy policy? When you are online, do you think of yourself as anonymous? Why or why not?

2. Do you agree with the Court that monitoring someone's online activity would reveal deeply personal and private information? Could it reveal information that was sensitive, but not illegal?

3. Before *Spencer* it had become commonplace for police to obtain identifying information about Canadians from ISPs. What is the harm in allowing the police to continue that practice in cases such as this?

4. In your opinion, will police investigations of similar cases be significantly delayed because they must apply for a search warrant?

5. The SCC was convinced that the seriousness of the offence was enough to include the evidence at trial, even though it was obtained unlawfully. In your opinion, should this be true of other anonymous cyber-crimes, like harassment, identity theft or leaking classified documents? Explain.