
CANADA / JUDGMENT

R. v. Caza

2015 BCCA 374

COURT

British Columbia Court of Appeal

DECIDED

28 August 2015

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

2015 BCCA 374 R. v. Caza

COURT OF APPEAL FOR BRITISH COLUMBIA

Citation:

R. v. Caza,

2015 BCCA 374

Date: 20150828

Docket: CA40234

Between:

Regina

Respondent

And

David James Caza

Appellant

Before:

The Honourable Madam Justice Bennett

The Honourable Madam Justice Garson

The Honourable Madam Justice Stromberg-Stein

On appeal from: An order of the Supreme Court of British Columbia, dated August 16, 2012 (R. v. Caza, 2012 BCSC 627, Kamloops Docket 89263).

Counsel for the Appellant:

E. Purtzki

Counsel for the Respondent:

M.A. Mereigh

Place and Date of Hearing:

Vancouver, British Columbia

April 1, 2015

Place and Date of Judgment:

Vancouver, British Columbia

August 28, 2015

Written Reasons by:

The Honourable Madam Justice Stromberg-Stein

Concurred in by:

The Honourable Madam Justice Bennett

The Honourable Madam Justice Garson

Summary:

Mr. Caza was convicted of child pornography offences and breach of a recognizance. The police had searched his home pursuant to a warrant and discovered a hard drive containing child pornography. The warrant was based largely on information obtained by the police through a request for subscriber information from the Internet service provider that owned the Internet protocol address associated with the Internet account used by Mr. Caza to transmit files to an undercover officer. The trial judge held that Mr. Caza had no expectation of privacy in the subscriber information under s. 8 of the Charter, and that even if he did, the evidence should not be excluded under s. 24(2) of the Charter. Mr. Caza appeals both findings in light of the recent Supreme Court of Canada decision, *R. v. Spencer*, 2014 SCC 43. Held: Appeal dismissed. Mr. Caza had no reasonable expectation of privacy in the subscriber information associated with the IP address.

Reasons for Judgment of the Honourable Madam Justice Stromberg-Stein:

Introduction

- [1] The appellant, David James Caza, was found guilty of possession of child pornography, contrary to s. 163.1(4) of the Criminal Code; transmitting or making available or distributing child pornography, contrary to s. 163.1(3); and breach of a s. 810.1 recognizance by engaging in, or attempting to engage in, any activity that involved contact with persons under the age of 16, including by use of a computer, contrary to s. 811.

- [2] Following the appellant's trial, the Supreme Court of Canada released reasons in *R. v. Spencer*, 2014 SCC 43. *Spencer* established that there was a reasonable expectation of privacy in the Internet Service Provider's subscriber information. *Spencer* held that a police officer's request for subscriber information amounted to a search. This forms the basis of Mr. Caza's appeal.

Facts

- [3] In 2009, Detective Paul Krawczyk, a police officer with the Child Exploitation Section of the Toronto Police Service, was an undercover user on an Internet network called "GigaTribe". GigaTribe is a peer-to-peer file-sharing network that is used for sharing child pornography. Once accepted as a member, GigaTribe users may share and download files, as well as send messages through a chat function. Users of GigaTribe are not required to provide any identifying information, and may remain completely anonymous, being known only by their username.
- [4] Detective Krawczyk's investigations led to the arrest of a GigaTribe user in Newfoundland. Utilizing that user's username and password, he made contact with Dan Quail who lived in the United States. As a result of this contact, Mr. Quail was arrested and the United States authorities provided Detective Krawczyk with Mr. Quail's GigaTribe username and password.
- [5] Detective Krawczyk logged into Mr. Quail's account and discovered a number of messages referencing child pornography from a GigaTribe contact named Paper123boy. The next day messages arrived from Paper123boy offering to share files. Detective Krawczyk reviewed thumbnail images of these files and discovered they contained child pornography. At the same time, Detective Krawczyk used software to capture both the thumbnail images and the Internet Protocol (IP) address for Paper123boy. He then used another website to determine that Shaw Communications Inc. (Shaw) was the Internet Service Provider (ISP) that owned the IP address.
- [6] Detective Krawczyk sent a "law enforcement request" to Shaw, indicating he was a police officer investigating child pornography offences on the Internet and requesting voluntary disclosure of the customer's name and address associated with the IP address.
- [7] Shaw complied with the request and informed Detective Krawczyk that the IP address belonged to Brian Feltham, who lived at #34, 110 Columbia Street in Kamloops, B.C.
- [8] Mr. Feltham had briefly resided with David James Caza at this address. When he moved, he cancelled his Shaw account. Unbeknownst to him, Mr. Caza reinstated it by purporting to be Mr. Feltham, had claimed to be him in all future dealings with Shaw, and had paid for the service. The Kamloops RCMP determined that Mr. Caza, who was known to them, resided at that address.

- [9] Based in large part on the information gathered by Detective Krawczyk, the RCMP prepared the information to obtain a search warrant (ITO) for Mr. Caza's residence. Mr. Caza was arrested at his residence. The police searched the residence twice pursuant to search warrants. The second search yielded a 500 gigabyte hard drive containing thousands of images and videos of child pornography.

The s. 8 Charter Voir Dire and Trial Judgment

- [10] Mr. Caza applied to exclude the hard drive seized during the second search, arguing that the ITO was based on information obtained through two unlawful searches, in violation of his rights under s. 8 of the Charter: *R. v. Caza*, 2012 BCSC 525.
- [11] First, he argued that by posing as Paper123boy's contact and downloading information from the account of Paper123boy, the police had conducted an unlawful search of Mr. Caza's computer. The judge rejected this argument and it is not appealed.
- [12] Second, Mr. Caza argued that his s. 8 rights were breached when the police requested the IP subscriber information from Shaw without a warrant. The judge rejected this argument and further noted that the fact Mr. Feltham's name was on the account was not significant: at para. 116.
- [13] The judge found that Mr. Caza had no reasonable expectation of privacy in the subscriber information associated with the IP address and that the terms of the agreement between Mr. Feltham and Shaw supported this conclusion: at paras. 50-56 and 115. He referred to several cases, including *R. v. McNeice*, 2010 BCSC 1544, which he found contained a similar Internet service agreement, where the Court held that the terms of the agreement supported that there was no expectation of privacy because the use of the service for dealing with obscene communications was prohibited and allowed the ISP to disclose customer information to the police where the service was being used in violation of the agreement.
- [14] The judge concluded that in responding to a police request for customer information under the Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5 [PIPEDA], an ISP does not become an agent of the state. He reasoned that an ISP "is really in the position of any other member of the community who is simply asked for information from the police and then provides it. The request does not amount to a search": at para. 51. Further, he held:
- [56] the terms of the contract between Shaw and the holder of the account make it clear that the holder of the account had no reasonable expectation of privacy with regard to his name and address where the police are making the request pursuant to PIPEDA. The joint terms of service and acceptable use policies and privacy policies were exhibited before me. The terms of service are subject to the Shaw acceptable use policies, and allow Shaw to disclose any information necessary to satisfy any legal regulatory or other governmental request. The acceptable use policy allows Shaw to cooperate with law enforcement authorities in the investigation of suspected criminal violations. This includes Shaw providing a user name, IP

address or other identifying information about the subscriber. The privacy policy that is part of the Shaw agreement does refer to PIPEDA.

- [15] Having found that Mr. Caza had no expectation of privacy, the trial judge held that Detective Krawczyk's request for the subscriber information therefore "was not a warrantless search and was not an unreasonable search": at para. 147.
- [16] The trial judge determined that if there was a breach of s. 8 of the Charter, the evidence obtained from the searches should not be excluded under s. 24(2). He found that any breach was not serious, and with respect to the police request for information from Shaw, "the process followed by the officer was consistent with additional authority at that time": at paras. 131-132. The judge did not address the impact of the state's Charter-infringing conduct on Mr. Caza's s. 8 rights in relation to the Shaw request. He found that society's interest in adjudicating the case on its merits supported the evidence's inclusion. He rejected Mr. Caza's argument that informed members of society would be concerned about the intrusion of state agents "into the most private regions [of] 'cyber space'", and that a failure to exclude the evidence "would run the risk of condoning such interference": at paras. 143-144.
- [17] In convicting Mr. Caza, the judge concluded, "Mr. Caza was the person who had possession of the hard drive, and was the person using that hard drive for the purposes of sharing the child pornography with other people": *R. v. Caza*, 2012 BCSC 627 at para. 93.

Issues on appeal

- [18] The issues on appeal arise under the umbrella of Mr. Caza's reasonable expectation of privacy. I will re-state the issues as follows:
1. Did the trial judge err in finding that the fact Mr. Feltham's name was on the account was not significant?
 2. Did the trial judge err in finding that there was no reasonable expectation of privacy in the subscriber information associated with Mr. Caza's IP address?
 3. Did the trial judge err in failing to exclude the evidence obtained through the search of Mr. Caza's residence under s. 24(2) of the Charter?

R. v. Spencer

- [19] In *Spencer*, the police were investigating child pornography offences using publicly available software to identify users sharing child pornography through a peer-to-peer file-sharing program. A police officer determined the IP addresses of several users who were sharing what he believed to be child pornography. Acting pursuant to PIPEDA and without obtaining prior judicial authorization, the officer asked the ISP to volunteer the subscriber information associated with an IP address that appeared to be located within his jurisdiction. The account belonged to Mr. Spencer's sister who, it was later determined, had

given him permission to use the account. The police used the subscriber information to obtain a search warrant for the sister's home where the accused lived. His computer was seized and subsequently searched, leading to the discovery of 50 child pornography images and two videos.

- [20] Mr. Justice Cromwell, writing for a unanimous court, considered whether the police officer's request for subscriber information amounted to a search, which required an analysis of whether the accused had a reasonable expectation of privacy in the totality of the circumstances: *Spencer* at para. 16. To answer this question, Cromwell J. considered four categories of factors: "(1) the subject matter of the alleged search; (2) the claimant's interest in the subject matter; (3) the claimant's subjective expectation of privacy in the subject matter; and (4) whether this subjective expectation of privacy was objectively reasonable": *Spencer* at para. 18, citing *R. v. Tessling*, 2004 SCC 67 at para. 32; *R. v. Patrick*, 2009 SCC 17 at para. 27; and *R. v. Cole*, 2012 SCC 53 at para. 40.
- [21] With respect to the subject matter of the search, Justice Cromwell took "a broad and functional approach to the question" looking "at not only the nature of the precise information sought, but also at the nature of the information that it reveals": *Spencer* at para. 26. Applying this approach, he found that the subject matter of the search was "not simply a name and address of someone in a contractual relationship with Shaw", but rather, was "the identity of a subscriber whose Internet connection is linked to particular, monitored Internet activity": *Spencer* at paras. 31-33.
- [22] Regarding the nature of the privacy interest engaged, Cromwell J. held that it was primarily informational, and in particular an interest in anonymity, but also territorial due to the fact that the accused used his home computer to share files: *Spencer* at paras. 37-48. He found that a user may have a Charter protected privacy interest in anonymity, depending on the totality of the circumstances. He concluded that the police request in *Spencer* attempted to link the suspect with anonymously undertaken online activities, information in which the accused had a direct and personal privacy interest: paras 50-51.
- [23] As to Mr. Spencer's subjective expectation of privacy, Justice Cromwell concluded the accused had a subjective expectation of privacy that could be readily inferred from his use of the network connection to transfer sensitive information: *Spencer* at para. 19.
- [24] In considering whether Mr. Spencer's expectation of privacy was objectively reasonable, Justice Cromwell noted that the contractual and statutory framework was relevant to, but not determinative of, the matter: *Spencer* at para. 54. The trial judge had found that there could be no reasonable expectation of privacy given the PIPEDA and the agreement between the accused's sister and the ISP. However, Cromwell J. concluded that if anything, the agreement created the overall impression that disclosure to the police would only be made where required or permitted by law: *Spencer* at para. 65. Justice Cromwell concluded that the accused had a reasonable expectation of privacy in the subscriber information, the request amounted to a search, and the police had no lawful authority for that search:

Spencer at paras. 66 and 69. In particular, Cromwell J. rejected the Crown's argument that the operation of s. 487.014 of the Criminal Code, which permits a police officer to make enquiries for voluntary production of documents, data or information, and s. 7(3)(c.1)(ii) of PIPEDA, which permits disclosure of personal information to a government institution pursuant to a lawful authority, authorized the police to make the law enforcement request of Shaw. He found that the accused's s. 8 Charter rights were therefore breached but concluded, following the application of the test in *R. v. Grant*, 2009 SCC 32, that exclusion of the evidence under s. 24(2) of the Charter would bring the administration of justice into disrepute: Spencer at para. 81.

Reasonable Expectation of Privacy

1. Did the trial judge err in finding that the fact Mr. Feltham's name was on the account was not significant?
- [25] The Crown argues that Mr. Caza had no reasonable expectation of privacy because, unlike Spencer, Mr. Caza did not have the permission of Mr. Feltham to use his Shaw account and therefore did not have a subjective or objectively reasonable expectation of privacy. In support of this argument, the Crown in its supplemental factum points to the following evidence:
 - (i) the appellant was supervised under a recognizance restricting his use of computers and prohibiting child pornography activities;
 - (ii) the appellant intentionally avoided setting up an Internet account in his own name;
 - (iii) the appellant accessed the Internet first through [a neighbour's] "splicing" an Internet cable to his apartment;
 - (iv) then, to have high speed access to allow for faster downloading capability, the appellant had Brian Feltham set up an Internet account; and
 - (v) prior to moving out, Brian Feltham ended the Internet service with Shaw, but the appellant, utilized Mr. Feltham's identity and continued the service without Mr. Feltham's knowledge or permission.
- [26] I agree with the Crown that the lack of permission from Mr. Feltham for Mr. Caza to use his Internet account is a material fact that distinguishes this case from Spencer.
- [27] Section 8 protects an individual from unreasonable search and seizure by the state where that person has a reasonable expectation of privacy: *Hunter v. Southam*, [1984] 2 S.C.R. 145 at 159. It protects people, not places, and relief for violations of s. 8 extends only to persons whose rights are infringed: *R. v. Edwards*, [1996] 1 S.C.R. 128 at para. 45.

- [28] As noted above, whether an individual has a reasonable expectation of privacy is determined by considering the totality of the circumstances, including the following four factors: (1) the subject matter of the alleged search; (2) the individual's interest in the subject matter; (3) the individual's subjective expectation of privacy in the subject matter; and (4) whether this subjective expectation of privacy was objectively reasonable: *Spencer* at para. 18, citing *Tessling*, *Patrick*, and *Cole*.
- [29] In *Edwards* at para. 45 the Supreme Court of Canada identified factors that relate to whether a person has a direct interest in the subject matter of the search, including possession or control of the property or place searched; ownership of the property or place; and historical use of the property or item. Although a possessory or proprietary interest is not required in order to establish a reasonable expectation of privacy, the fact that a person was unlawfully in the place searched can undermine a reasonable expectation of privacy: see *R. v. Lauda*, [1998] 2 S.C.R. 683 at para. 1, citing *Edwards* and *R. v. Belnavis*, [1997] 3 R.C.S. 341.
- [30] The Court in *Spencer* briefly dealt with the issue of whether the claimant had a direct interest in the subject matter of the search, finding that "[t]hough he was not personally a party to the contract with the ISP, he had access to the Internet with the permission of the subscriber and his use of the Internet was by means of his own computer in his own place of residence": at para. 19. (Emphasis added.)
- [31] As in *Spencer*, Mr. Caza's subjective expectation of privacy "can readily be inferred from his use of the network connection to transmit sensitive information": *Spencer* at para. 19. Mr. Caza was "personally and directly exposed to the consequences of the police conduct"; that is, warrantless surveillance of his Internet activity in his own home on his own computer. This "specifically observed, anonymous Internet activity engages a high level of informational privacy": *Spencer* at para. 51.
- [32] In my view *Spencer* is distinguishable. Although Mr. Caza had a direct interest in the subject matter of the search, including an informational privacy interest of anonymity in the subscriber information linking him to his particular, monitored Internet activity, and a territorial privacy interest resulting from his use of his home computer, and he may have had a subjective expectation of privacy, his subjective expectation was not objectively reasonable. Mr. Caza did not have the permission of Mr. Feltham to use his Shaw account and, in fact, fraudulently hijacked his Internet account. Lack of permission in the circumstances of this case is sufficient to render any subjective expectation of privacy Mr. Caza may have had objectively unreasonable.
- [33] Mr. Caza had no reasonable expectation of privacy in the subscriber information associated with the IP address the disclosure of which led to a search of Mr. Caza's Internet activities in his own home. This ground of appeal must fail. This conclusion also addresses the second ground of appeal; that is, that there was no error in finding that there was no reasonable expectation of privacy in the subscriber information associated with the IP address. Having found no Charter breach I do not have to deal with the trial judge's alternate conclusion on

whether the evidence obtained through the search of Mr. Caza's residence was admissible under s. 24(2) of the Charter.

Conclusion

[34] I would dismiss the appeal.

"The Honourable Madam Justice Stromberg-Stein"

I agree:

"The Honourable Madam Justice Bennett"

I agree:

"The Honourable Madam Justice Garson"

Source & reproduction note

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

ORIGINAL SOURCE <https://www.bccourts.ca/jdb-txt/CA/15/03/2015BCCA0374.htm>

CASE PAGE <https://chat.esheria.ai/case-law/canada/r-v-caza-2015>

Prepared on 28 October 2026 · Esheria