COURT FILE NO.: 4191/08
DATE: 2009-02-10

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:	)	
	)	
HER MAJESTY THE QUEEN	)	Elizabeth A. Maguire, for the Respondent
	)	
	)	
Respondent	)	
	)	
- and -	)	
	)	
MILES WILSON	)	Ron Ellis, for the Applicant
	)	
	)	
Applicant	)	
	)	**HEARD:** December 10, 2008 at St. Thomas.

R U L I N G

LEITCH R.S.J.:

[1] The applicant is charged with unlawfully possessing and unlawfully making available child pornography contrary to sections 163.1(3) and 163.1(4) of the *Criminal Code of Canada*, R.S.C. 1985, c. C-46. The issue on this application is whether the police are required to obtain a warrant before requesting a subscriber's name and address from an internet service provider.

[2] The applicant claims a reasonable expectation of privacy in information obtained from Bell Canada, his wife's internet service provider. It is argued by the applicant that his rights under s. 8 of the *Canadian Charter of Rights and Freedoms* were violated because the police failed to obtain a warrant before requesting the name and address of the account holder of an IP address. As a result, it is the applicant's position that while the warrant authorizing the search of his home appears valid on its face, the application for that warrant was based on information obtained in violation of his s. 8 rights. Accordingly, it is claimed that the admission of evidence obtained when the search warrant was executed will bring the administration of justice into disrepute.

[3] Section 8 of the *Charter* guarantees that citizens are to be free from unreasonable search and seizure and states, "everyone has a right to be secure against unreasonable search or seizure."

[4] The investigating officer, Officer Schmidt, did what is described as a "plain view search" on the internet of what is available to be seen in the public domain, and procured an IP address. As Officer Schmidt testified, it is possible for someone to Google how to find an IP address on the internet and the information to determine who owns that address, in this case Bell Canada, is also publicly available.

[5] Officer Schmidt sent a letter by facsimile to Bell Canada requesting account information pursuant to a child sexual exploitation investigation. Specifically, he requested the last known customer name and address of the account holder associated with a specific IP address used on April 12, 2007 at 9:26 a.m. eastern daylight time. The letter indicated that disclosure was requested in accordance with s. 7(3)(c.1) of the *Personal Information Protection Electronic Documents Act*, S.C. 2000, c. 5 ("*PIPEDA*"), and that his authority to request and obtain the information derived from his appointment as a police officer under the *Police Services Act*, R.S.O. 1990, c. P-15 (this same language was contained in the search analyzed by the court in *Kwok, infra*).

[6] Officer Schmidt did not draft the letter to Bell Canada. He simply filled in the blanks of what he referred to as a "standard letter." His letter did not indicate that he needed to locate a computer or that there was any emergency or that he required the information immediately.

[7] Officer Schmidt did not have a warrant to obtain the information, but Bell Canada nonetheless complied with his request, and on Friday, April 13, 2007 at 2:35 p.m provided him with the name "Janet Wilson 105 Sunset Drive, St. Thomas, Ontario N5R 3B5."

[8] On April 16, 2007, Officer Schmidt conducted a background investigation on the name Janet Wilson and the home address provided by Bell Canada. He conducted a Versadex check (a computer system designed primarily to enhance the operational and reporting functions of the London City Police Service) and a CPIC check on Janet Wilson. He also conducted a Ministry of Transportation check on Janet Wilson with the birth date he obtained from his Versadex check. Further, after contact with a constable of the St. Thomas Police Service, he received information as to the occupants of 105 Sunset Drive which included the applicant. He then conducted a CPIC check, Versadex check and Ministry of Transportation check on the applicant. He conducted a Canada411.ca internet search on M. Wilson of St. Thomas and located a listing for an M. Wilson at 105 Sunset Drive, St. Thomas, Ontario along with a telephone number, both of which were consistent with the information provided by the St. Thomas Police Service.

[9] On April 19, 2007 Officer Schmidt swore an affidavit in support of a search warrant in which he deposed that he verily believed that he had reasonable grounds to believe that the granting of the search warrant for the residence of Janet Wilson located at 105 Sunset Drive, St. Thomas, Ontario would afford evidence with respect to the offences of possession of child pornography and making available child pornography contrary to sections 163.1(3) and 163.1(4) of the *Criminal Code of Canada*.

The Privacy Right Guaranteed by s. 8 of the *Charter*

[10] Section 8 of the *Charter* guarantees protection from unreasonable searches. The case law is clear that the protection of individual privacy must be balanced by the need to achieve social

protections. The need for this balance was enunciated by Binnie J. in *R. v. Tessling*, [2004] S.C.R. 432 [*Tessling*], at para. 17:

> At the same time, social and economic life creates competing demands. The community wants privacy but it also insists on protection. Safety, security and the suppression of crime are legitimate countervailing concerns. Thus s. 8 of the *Charter* accepts the validity of reasonable searches and seizures. A balance must be struck ...

[11] Binnie J. in *Tessling* turned to *Hunter v. Southam Inc.*, [1984] 2 S.C.R. 145, where at page 159 Dickson J. stated that "such balancing between individual rights and social or governmental goals means: the guarantee of security from unreasonable search and seizure only protects a reasonable expectation."

[12] And in *R. v. Edwards*, [1996] 1 S.C.R. 128, Cory J., writing for the majority, summarized the principles that ought to be considered in assessing whether an individual had a reasonable expectation of privacy such that the possibility of a s. 8 violation could be explored. He provided the following guidelines at para. 45:

> 1. A claim for relief under s. 24(2) can only be made by the person whose *Charter* rights have been infringed.
>
> 2. Like all *Charter* rights, s. 8 is a personal right. It protects people and not places.
>
> 3. The right to challenge the legality of a search depends upon the accused establishing that his personal rights to privacy have been violated.
>
> 4. As a general rule, two distinct inquiries must be made in relation to s. 8. First, has the accused a reasonable expectation of privacy? Second, if he has such an expectation, was the search by the police conducted reasonably?
>
> 5. A reasonable expectation of privacy is to be determined on the basis of the totality of circumstances.
>
> 6. The factors to be considered in assessing the totality of the circumstances may include, but are not restricted to, the following:
>
> (i) presence at the time of the search;
>
> (ii) possession or control of the property or place searched;
>
> (iii) ownership of the property or place;
>
> (iv) historical use of the property or items;
>
> (v) the ability to regulate access, including the right to admit or exclude others from the place;

(vi) the existence of a subjective expectation of privacy;

(vii) the objective reasonableness of the expectation.

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

[13] Therefore the "totality of the circumstances" must be examined in order to make an assessment whether an individual had a reasonable expectation of privacy and in such an examination the form of the privacy ought to also be considered.

[14] While privacy of the person and the presumption of bodily integrity typically attracts the most serious expectations of privacy (see *Tessling* para. 21), two other forms of privacy – territorial and biographical – can also attract s. 8 protection, and include "informational privacy." As stated by Binnie J. in *Tessling* at para. 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.

[15] Informational privacy was at issue in *R. v. Plant*, [1993] 3 S.C.R. 281 [*Plant*], where the Supreme Court of Canada considered whether police access to an individual's electricity consumption required a warrant. Sopinka J., for the majority, concluded at para. 20 that an examination of electrical records did not require a warrant:

> In fostering the underlying values of dignity, integrity and autonomy, it is fitting that s. 8 of the *Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This would include information which tends to reveal intimate details of the lifestyle and personal choices of the individual. The computer records investigated in the case at bar while revealing the pattern of electricity consumption in the residence cannot reasonably be said to reveal intimate details of the appellant's life since electricity consumption reveals very little about the personal lifestyle or private decisions of the occupant of the residence.

[16] Therefore, in order to assert an expectation of privacy in personal information, that personal information must be biographical in nature, revealing particulars and specifics about the life and interests of the individual in question.

Position of the Applicant

[17] The applicant submits that the warrant to search his home was unlawfully obtained due to the fact the police did not obtain a judicial warrant to acquire the private information from Bell Canada initially required to obtain the search warrant. The applicant asserts that a reasonable person would feel the evidence ultimately obtained as a result of this breach should be excluded.

[18] The applicant relies on the recent decision of Gorewich J. in *R. v. Kwok*, [2008] O.J. No. 2414 (Ct. Jus.) [*Kwok*], and urges me to make a similar finding.

[19] The applicant notes that Officer Schmidt acknowledged that at no point did he and the applicant engage in online communication. There was neither email between them nor any online chat. Officer Schmidt also did not search a chat room to find the applicant. The applicant did not invite Officer Schmidt to see any photos or vice versa. The applicant submits that these circumstances suggest a greater expectation of privacy.

[20] The applicant notes there is direct evidence that Janet Wilson had a privacy concern with respect to her phone and internet service and no indication she read or signed the internet service agreement that limited her privacy interest. Janet Wilson contracted with Bell Canada for a "bundled" phone and internet service. She testified that she did not recall seeing and thus did not read the Bell Sympatico High Speed Internet Service Agreement which came up on her computer screen when the internet service was set up. She acknowledged she would have clicked a box indicating her acceptance of that agreement.

[21] Janet Wilson testified that the phone book listing "M. Wilson" is not the applicant's listing but rather is her listing with "M" standing for her middle name. She testified that she had such a listing to resolve her privacy concerns arising from her employment at St. Thomas Psychiatric Hospital. She testified that she had the same privacy concerns with respect to her internet service.

[22] In *Kwok* at paras. 13 and 14 the court concluded that as a matter of common sense there can be an expectation of privacy for those, other that the subscriber, in the same household using the equipment which is in the subscriber's name. The applicant here asserts that it is common sense that he and his spouse had the same expectation of privacy.

[23] The applicant further asserts that the police contacted Bell Canada without prior judicial authorization simply to speed up the investigation. Indeed the applicant takes the position that a certain exigency was suggested by the reasons indicated for seeking the information, and as a result Bell Canada would have felt compelled to provide the information.

Position of the Crown

[24] The crown acknowledges that Janet Wilson testified that she did have an expectation of privacy in her phone number. However, the crown submits that it defies belief that she would endeavour to hide behind a listing showing her address, her surname and the same initial as her husband because there are far more effective ways to secure her privacy in the phone book. The crown's position is that her stated expectation of privacy is not credible and, in any event, it is vitiated by the terms of her contract with Bell.

[25] However, the crown submits the important issue is whether the applicant had any reasonable expectation of privacy. In that regard the crown submits that the applicant has not established that he had such expectation in the information Bell gave to the police because the personal information disclosed was not the applicant's.

[26] Further, the crown emphasizes that the police officer simply obtained the name and address of a person using a particular IP address and this information is not biographical core information in which one would expect to have a privacy interest. The crown queries how one could have a reasonable expectation of privacy in information that is also listed in a public directory and analogizes this case to the Superior Court decision of *Edwards, infra* where cell phone records were obtained.

[27] Finally, the crown submits that even if there was a s. 8 breach, it was not a serious breach and would not require the evidence to be excluded.

Is there a reasonable expectation of privacy in ISP subscriber information?

[28] The onus is on the applicant to establish on a balance of probabilities that he had an expectation of privacy with respect to the information obtained from Bell Canada – that is, his wife's name and address. According to her evidence, Janet Wilson did have such an expectation of privacy in her phone number.

[29] The first issue on this application is whether the applicant could have a reasonable expectation of privacy in his wife's information. Or, to put it another way, does the applicant have standing to challenge the search in issue? Does the fact that the applicant did not enter into the contract with Bell Canada lead to the conclusion that he had no reasonable expectation of privacy in the information disclosed by Bell Canada?

[30] In *R. v. Edwards*, [1999] O.J. No. 3819 (S.C.J.) [*Edwards*], the investigating officer obtained a subscriber's name and address and a user's name and residential telephone number to which a cell phone number was registered. As it happened, the latter registered information belonged to the mother of the eventual accused and LaForme J. as he then was commented that the accused would not have any expectation of privacy in such information because it was his mother's information and was listed in the public telephone directory.

[31] However, I concur with the approach in *Kwok* as earlier referred to which was expanded upon in *Friers, infra*, at para. 19 as follows: "where the utility is one that all members of a household will likely use the fact that the defendant did not formally enter into a contract with the utility supplier does not preclude him from having standing to claim a s. 8 breach (see *R. v. MacInnis*, [2007] O.J. 2930 (S.C.J.). at [52]-[54] and *R. v. Kwok*...)." This reasoning is in keeping with Bell's definition of "customer" in its Code of Fair Information Practices as including "an individual who uses... the products or services of a Bell company."

[32] The issue of whether subscriber information maintained by a wireless phone service merited s. 8 protection was considered in *Edwards*. An investigating officer obtained through a phone company the name and address to which a cell phone number was registered. LaForme J. held that the police did not require a warrant to obtain such information and there was no s. 8 violation. He agreed with the crown submission that Mr. Edward's could not have any expectation of privacy in his name and address because the service agreement provided that such information would not be kept confidential. In addition, he held following *Plant* and *R. v. Lillico* (1994), 92 C.C.C. (3d) 90 (Ont. Gen. Div.), that while a third party commercial enterprise ought

to be expected to maintain privacy in confidential customer information, that information would not include subscriber names and addresses. He stated the following at para. 37:

> Cantel has, and indeed recognizes, its duty to keep personal information of its customers confidential; however it needs only to do so in respect of that information which tends to reveal intimate details of the customer's personal lifestyle and choices. The subscriber's name and address do not fall within this category. This is simply the general information that all persons engaging in commercial contractual relations accept. Moreover, it is not information that anyone has, in such commercial relations as this, any expectation of privacy in.

[33] Similarly, in *R. v. Stucky*, [2006] O.J. No. 108 (S.C.J.), Gans J. found that subscriber information with respect to a post office box did not merit a reasonable expectation of privacy attracting s. 8 protection.

[34] The reasoning in *Edwards* was applied in *R. v. Ward*, [2008] O.J. No. 3116 (O.C.J.), where Lalande J. concluded that a warrant was not necessary in order to obtain a subscriber's name and home address attached to an IP account. As Lalande J. stated at para. 68:

> In this case, the 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 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.

[35] In this case, as in *Ward*, Bell Canada was the internet service provider and its Code of Fair Information Practices permits Bell to "disclose personal information without knowledge or consent ...to comply with a subpoena, warrant or other court order, or as may be otherwise required by law" and the "use of products and services by a customer...constitutes implied consent for the Bell Companies to collect, use and disclose personal information for all identified purposes". Personal information is defined to include "a customer's credit information, billing records, service and equipment, and any recorded complaints". As Lalande J. observed in *Ward*, this service agreement "contemplates disclosure which is more intrusive than a subscriber's simple name and address."

[36] Similarly, in *R. v. Friers*, Information No. 07-424 released September 17th, 2008 (O.C.J.) [*Friers*], Nadel J. held that account information such as a subscriber's name and address was not protected by s. 8. As he concluded in para. 24:

> Account information per se reveals very little about the personal lifestyle or private decision of the occupants of the defender's residence other than they have chosen to have some form of internet connection installed in that residence.

...

Like Lalande J. in *R. v. Ward*, I conclude that subscriber information is not core personal information.

[37] However, the applicant urges me to reach a conclusion consistent with Gorewich J. in *Kwok* who held that the accused's s. 8 rights were violated when, after obtaining the accused's IP address, the police approached his internet service provider for the account holder's name and address. As is the case here (and as it was in *Ward* and *Friers)* the request was made under s. 7(3)(c.1) of *PIPEDA*. Gorewich J. concluded there was a reasonable expectation of privacy in subscriber information. He considered the police reliance on *PIPEDA* to be a shortcut and concluded they ought to have obtained a warrant.

[38] With respect to this latter point, in my respectful view, it is not accurate to say that *PIPEDA* is a shortcut. The purpose of *PIPEDA* is set out in s. 3 as follows:

> 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.

[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. Section 7(3)(c.1)(ii) of *PIPEDA* provides as follows:

> 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 relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law.

[40] Officer Schmidt made a request under the authority of the *Police Services Act* and Bell Canada was permitted to release the information under s. 7(3)(c.1) of *PIPEDA*. Therefore, both the police officer's request and Bell Canada's response was authorized. Bell Canada had the right to refuse the request and such refusal would have required Officer Schmidt to obtain a warrant. I do not find that the contents of the letter of request represented that the circumstances underlying the request were exigent thus imposing some sense of urgency or obligation on Bell Canada.

[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 occupant's of the defendant's residence other than they have chosen to have some form of internet connection installed in that residence. Moreover, the prevalence of wireless and handheld technology makes a particular address an even less significant fact so far as internet use is concerned, since that use is no longer tied to a land line tied to a particular address.

[43] In addition, in this case the terms of the contract with the internet provider is one of the factors to be considered in assessing whether the asserted expectation of privacy is reasonable in the totality of the circumstances. That contract includes an agreement that the service provider could disclose any information necessary to satisfy any laws, regulations or other governmental request from any applicable jurisdiction. Further, the agreement contained a provision that by subscribing to the service, one consents to the collection, use and disclosure of personal information as described in the Bell Customer Privacy Policy and the Bell Code of Fair Information Practices. This privacy statement includes a provision that Bell Canada may also provide personal information to law enforcement agencies. Therefore by virtue of the contractual terms on which the internet service was provided an expectation of privacy is not reasonable.

[44] Accordingly, I find that there has been no breach of the applicant's s. 8 rights.

Regional Senior Justice Lynne C. Leitch

Released: February 10, 2009.

Court File No.: 4191/08
Date: February 10, 2009.

ONTARIO
SUPERIOR COURT OF JUSTICE

B E T W E E N:

HER MAJESTY THE QUEEN

Respondent

- and -

MILES WILSON

Applicant

R U L I N G

LEITCH R.S.J.

Released: February 10, 2009.