“1984” in 2009: R. v. Wilson

In the recent case of *R. v. Wilson*, the Ontario Superior Court of Justice held that a person’s account information linked to an internet provider’s address (IP address) was not subject to the reasonable expectation of privacy; therefore, police do not require a warrant to gain this information, and there is no violation of section 8 of the *Charter of Rights and Freedoms* if IP addresses are collected by police. Section 8 of the *Charter* states that “everyone has a right to be secure against unreasonable search and seizure.”[1]

The case concerned an application to rule out evidence that the applicant argued had been acquired by an unreasonable search and seizure. While conducting a routine search of the Internet, a police officer came across child pornography in an open forum. Using techniques available to anyone on the Internet, the officer proceeded to obtain the IP address connected with the online child pornography in question.[2] The officer then made an application to Bell Canada, using a standard form in which the officer applied for the name and address belonging to the IP account holder.[3] Bell then relayed the information requested to the officer conducting the investigation.[4] After receiving the name and address of the account holder, who in this case was the applicant’s wife, the officer then obtained a search warrant for the household and proceeded to discover data archives of child porn.[5]

The sole issue before the court in this case was “whether the police are required to obtain a warrant before requesting a subscriber’s name and address from an Internet service provider.”[6] The court relied in part on the Supreme Court of Canada (SCC) decision in *R. v. Edwards*, where the SCC outlined a number of points to consider in assessing a section 8 *Charter* violation.[7] The most important question in this case was whether the accused had a reasonable expectation to privacy. The Ontario Superior Court found that in order for the accused to assert an expectation of privacy, the information must be of a biographical nature.[8] In the Ontario *Wilson* case, the court held that Bell giving out an account holder’s name and address (associated with an IP address) was not significantly different from publication of a name and address in a phone book.

In the Ontario court’s rejection of the application for the exclusion of evidence gathered as a result of the IP-linked information, it made a hotly contested judgment that IP addresses were not “biographical” in nature; therefore, police do not require a search warrant to attain that information. But as many critics have pointed out, an IP address can be used to trace an individual’s entire online history.[9] By allowing an IP address to be linked to an individuals name, it effectively allows for the construction of an electronic biography that can be revealing and potentially damaging.

In arriving at the conclusion that Mr. Wilson could not have reasonably expected his information to remain private, the court relied in part on the contract his wife had signed with Bell. The contract stated that Bell was allowed to "disclose personal information without the knowledge or consent of the subscriber."[10] This raises the further issue of whether *Charter* rights can be contracted away by a third-party.

Currently, Canadian legislation such as the *Personal Information Protection and Electronic Documents Act*(PIPEDA)[11] allows Internet providers to release customers' names and addresses without a search warrant.[12] It is worth comparing the United Kingdom (U.K.) experience, in which full electronic citizenry surveillance is common. Building upon a government initiative started a decade ago to establish closed circuit t.v. monitors (CCTV) in public spaces, the U.K. government has recently expanded the practice by making access to private CCTVs a precondition for business licenses is some cases.[13] Today there are more than 4.2 million CCTV's in the U.K., monitoring almost every aspect of its citizens' daily activities.[14]

---

[1] *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 (CanLII).
[2] *R. v. Wilson* (10 February 2009), St. Thomas 4191/08 (ON Sup. Ct.) at para. 4, online: Canadian Privacy Law Blog .
[3] *Ibid*. at para. 5.
[4] *Ibid*. at para. 7.
[5] *Ibid*. at para. 8.
[6] *Ibid*. at para. 1.
[7] *R. v. Edwards*, [1996] 1 S.C.R. 128 at para. 45 (CanLii).
[8] *Supra* note 2 at para. 16.
[9] Shannon Kari, "Where you've been on Net not private, judge rules" *National Post* (13 Feb 2009).
[10] *Supra* note 2 at para. 35.
[11]S.C. 2000, c.5.
[12] *Ibid*. at para. 39.
[13] Canadian Privacy Law Blog, "UK pub required to install CCTV to get police approval for liquor license" (10 February 2009).
[14] Richard Tyler, "UK is CCTV Capital" *ukwatch.net* (6 December 2006).