# • PRIVACY, TECHNOLOGY, AND INSTANT MESSAGING —THE BRITISH COLUMBIA COURT OF APPEAL SENDS A (INSTANT) MESSAGE •

Dara Jospé, Associate, Michael Shortt, Associate, and Antoine Guilmain, Articling Student, Fasken Martineau DuMoulin LLP


**Dara Jospé**

**Michael Shortt**

**Antoine Guilmain**

**In** its recent decision *R. v. Craig*, [2016] B.C.J. 154, 2016 BCCA 154, the British Columbia Court of Appeal recognized a reasonable expectation of privacy in *private* instant messages shared on a social network. Even though the context was criminal law, the reasoning underlying the decision is of interest to any practitioner confronted with protection of privacy issues. This bulletin discusses this case first by presenting the facts, followed by the legal issues, the "reasonable expectation of privacy" test, and the court's guidance for the future.

## FACTS

This was a criminal case involving Internet luring of a minor. At the end of 2009, the appellant Mr. Craig (aged 22 years) entered into contact with the complainant E.V. (aged 13 years) through Nexopia instant messaging — a social networking website for teenagers. They subsequently met and eventually had sexual relations. The police were informed of the situation and, in early 2010, conducted an investigation and obtained a search warrant for the data housed on Nexopia servers (in Alberta), the purpose of which was to establish the offence of Internet luring of a minor. Finally, only the messages from the account of the complainant E.V. (and her friends) were sent to the Crown, which was not the case for the messages of the appellant Mr. Craig. Based partly on this evidence, the British Columbia Supreme Court found Mr. Craig guilty on several counts of the offence under the *Criminal Code*.

## LEGAL ISSUES

Mr. Craig appealed this decision and asked the Court of Appeal to examine six grounds for appeal, including one on the right to privacy. Mr. Craig felt that his reasonable expectation to privacy had not been given as much consideration as that of the complainant E.V. He argued that the trial judge applied a double standard by characterizing the instant messages sent via Nexopia differently: on the one hand, they were *private* for the complainant pursuant to section 278.3 of the *Criminal Code*, and on the other, they were *public* for the appellant pursuant to section 8 of the *Charter of Rights and Freedoms*. The Court of Appeal noted and condemned this double standard regarding the right to privacy.

## REASONABLE EXPECTATION OF PRIVACY

A preliminary comment is called for at this point: the instant messages in question came and were seized from the accounts of the complainant E.V., not from that of Mr. Craig. As stated by the Court of Appeal, "Mr. Craig does not assert reasonable expectation of privacy in the accounts of E.V. and the other witnesses, just the messages found therein". That being said, the Court of Appeal, relying on a series of leading cases, held that Mr. Craig had a reasonable expectation of privacy in the instant messages sent to the complainant E.V., regardless of the Nexopia account from which these messages were retrieved. Numerous criteria led to this conclusion (subject matter of the search, claimant's interest, subjective expectation of privacy), but one warrants special attention: the *objective* reasonableness of the expectation.

Could Mr. Craig expect that the messages sent to the complainant would remain confidential? On the one hand, according to the doctrine of "loss of control" or "risk analysis", the sender abandons his right to privacy in the content of messages sent to the extent that he knows or should have known that the recipient might share them with anyone. This approach comes from the United States, and was the one applied by the trial judge. On the other hand, according to the doctrine of "confidentiality", the sender does not abandon his right to privacy in the content of the message to the extent that he can and should be able to count on the recipient's duty of confidentiality with respect to third parties. In this sense, and contrary to the trial judge, the Court of Appeal held that Mr. Craig was entitled to a reasonable expectation of privacy in the instant messages sent to the complainant E.V., since he was not supposed to know that the said messages would be shared with third parties. This approach does not deny the risk that a message will be disclosed; according to the Court of Appeal, that risk is inherent in any human interaction and depends on the relationship between the parties, the specific circumstances, and the nature of the said message. However, the Court of Appeal noted that the risk of improper sharing of a message (*i.e.* breach of confidentiality) is not enough to vitiate a reasonable expectation of privacy.

## PRIVACY VS TECHNOLOGY?

In our opinion, this decision can be summed up in two words as it pertains to reasonable expectation of privacy: tradition and progress. *Legal tradition*, because the Court of Appeal reiterated and affirmed the doctrine of confidentiality in private communications: the sender is not supposed to know that the recipient will share the message with third parties. *Technical progress*, because the Court of Appeal applied this doctrine, with the necessary adaptations, to the digital universe, by explaining that *private* instant messages shared on a social media website are entitled to an *objective* expectation of privacy. Most importantly, from a much broader perspective, this principle would apply to any *private* technological communication. The appellate judges, for example, drew numerous analogies with texts or emails, particularly in the following passage:

> [63] While recognizing that electronic surveillance is a particularly serious invasion of privacy, the reasoning is of assistance in this case. Millions, if not billions, of emails and "messages" are sent and received each day all over the world. *Email has become the primary method of communication. When an email is sent, one knows it can be forwarded with ease, printed and circulated, or given to the authorities by the recipient. But it does not follow, in my view, that the sender is deprived of all reasonable expectation of privacy*. I will discuss this further below. To find that is the case would permit the authorities to seize emails, without prior judicial authorization, from recipients to investigate crime or simply satisfy their curiosity. [Our emphasis]

The scope of this decision is therefore legal-technological, an attempt at reconciliation that must be noted and commended. However, while this decision is a promising beginning, the reasoning is not without its faults, in particular with respect to an examination of the technological process. The decision has surprisingly few "technical" references to the tool whose use was in question, namely the instant messaging system integrated

into the Nexopia social media website: Is there a maximum number of recipients for a message? Can other users be limited or excluded from entering the discussion? Is it possible to block responses to the conversation? The answers to this list of questions, based on a brief interaction with the Nexopia messaging service, significantly affects how the reasonable expectation of privacy will be analyzed. Further, and as a warning, note that (i) not all instant messaging systems are the same, (ii) not all instant messages are private communications and (iii) the private/public distinction depends more and more often on technological configurations. Therefore, and we cannot stress this enough, these cascading considerations call for a *functional approach* when determining the reasonable expectation of privacy.

[***Dara Jospé*** *is an associate at Fasken Martineau's Montreal office. She practices in the area of life sciences regulation and advises on all stages in the lifecycle of a pharmaceutical product from its initial conception until it reaches the consumer.*

***Michael Shortt*** *is an associate at Fasken Martineau's Montreal office. He has a general intellectual property practice, with a particular focus on patent and copyright litigation.*

***Antoine Guilmain*** *is a Ph.D. candidate in Information Technology Law and an articling student at Fasken Martineau's Montreal office. He is particularly interested in privacy and personal information protection, as well as electronic evidence, information security and intellectual property. He has published several works in these fields.*]