• THE FAKE FACEBOOK PROFILE AND THE VEILED VICTIM •

Margot Patterson
Fraser Milner Casgrain LLP

In *A.B. v. Bragg Communications Inc.*,[1] the Supreme Court of Canada determined that a 15-year-old can proceed anonymously to pursue the identity of her Facebook cyberbully.

Background

The 15-year-old, A.B., found out that someone had posted a fake Facebook profile with her picture, a modified version of her name, and other identifying particulars. The profile also included demeaning comments about A.B.'s appearance and sexually explicit references.

Facebook provided the IP address associated with the Nova Scotia account holder. The Internet provider, Eastlink, agreed to provide more specific information about the address if a court authorized it to do so. A.B. brought an application for such an order and, along with the application, requested (i) permission to seek the identity of the Facebook cyberbully anonymously (the "anonymity request") and (ii) a publication ban on the content of the fake Facebook profile.

While Eastlink did not oppose these privacy requests, the *Halifax Herald* and Global Television did. The Nova Scotia court granted the order requiring Eastlink to disclose the information about the identity of the cyberbully. However, it denied A.B.'s anonymity request and the publication ban on the basis that she had not proved specific harm to her that would outweigh restricting access to the media. Put simply, the media's right to access and report on the facts of the case outweighed A.B.'s right to privacy. This was upheld at the Nova Scotia Court of Appeal.

The Supreme Court Decision: Public Disclosure v. A Child's Privacy

A unanimous Supreme Court overturned this, stating that:

> If we value the right of children to protect themselves from bullying, cyber or otherwise, if common sense and the evidence persuade us that young victims of sexualized bullying are particularly vulnerable to the harms of revictimization upon publication, and if we accept that the right to protection will disappear for most children without the further protection of anonymity, we are compellingly drawn in this case to allowing A.B.'s anonymous legal pursuit of the identity of her cyberbully.[2]

The Supreme Court noted that the decision in *Canadian Newspapers Co. v. Canada (Attorney General)*[3] had established that the limits on the media's right to freedom of the press imposed by prohibiting identity disclosure in a criminal sexual assault case are minimal: the media can be present at the hearing and report facts and the conduct of the trial without revealing the complainant's identity.

In the *A.B.* decision, the Supreme Court placed great emphasis on the inherent vulnerability of children and the importance of protecting their privacy in the context of cyberbullying. In the view of the Supreme Court, if we accept that, then surely we must accept the need to prohibit identity disclosure in this case, just as the court did in the criminal context in *Canadian Newspapers*.

The Supreme Court allowed A.B.'s appeal in part: her identity and the identifying information in the fake Facebook profile would be protected. The non-identifying information in the profile could be disclosed.

Child-Specific Privacy Standards in Context

This decision provides further direction for those who are conscious of the protection of the privacy of children and who wonder about the specific content of those obligations. Unlike the United States, Canada has no *Children's Online Privacy Protection Act* [*COPPA*]. While there are set age and child-specific standards in Canadian criminal laws, we have no set age and child-specific standards in our federal privacy legislation, the *Personal Information Protection and Electronic Documents Act*.[4]

The Supreme Court noted that:

> Recognition of the *inherent* vulnerability of children has consistent and deep roots in Canadian law. This results in protection for young people's privacy under the *Criminal Code*, R.S.C. [...] the *Youth Criminal Justice Act* [...], and child welfare legislation, not to mention international protections such as the *Convention on the Rights of the Child* [...], all based on age, not the sensitivity of the particular child.

The court has sent a message that in contexts where children may be particularly vulnerable—even when the child is 15 years old, and the context is Facebook—the law will protect their privacy on an objective basis based on age, not individual maturity or temperament.

[*Editor's note*: **Margot Patterson** is Counsel with Fraser Milner Casgrain LLP. Margot is recommended by Best Lawyers in Canada 2013 as one of Canada's leading lawyers in the area of Communications Law. She blogs at <www.datagovernancelaw.com>.]

---

1 [2012] S.C.J. No. 46 (S.C.C.).

2 *Ibid.* at para. 27.

3 [1988] S.C.J. No. 67 (S.C.C.).

4 S.C. 2000, c. 5 [*PIPEDA*]. While the Office of the Privacy Commissioner of Canada ("OPC") has published useful presentations such as *Understanding Your Online Footprint: How to Protect Your Personal Information on the Internet*, available at <http://www.youthprivacy.ca/en/Presentation/Speaking_Notes_4-6_Youth_Presentation_Package_EN.pdf>, the OPC's standard statement referencing informed consent for the collection, use, retention, and disclosure of personal information from children is simply that "it is difficult to obtain meaningful consent from children."

• OWNERSHIP & POLICIES NOT DETERMINATIVE OF PRIVACY IN ELECTRONIC DEVICES •

Timothy M. Banks
Fraser Milner Casgrain LLP

Employee Privacy at Work

Are device ownership and acceptable use policies determinative of an employee's expectation of privacy?

Many employers attempt to diminish the expectations of privacy of employees in work-supplied electronic devices through "computer use" policies. These policies typically state that work-supplied devices are to be used solely for work purposes and that the employer may monitor the employee's use of these devices. These policies are perhaps honoured more in their breach with employees frequently accessing online banking, social networks, and other websites and online applications from workplace-supplied computers and smartphones.

Leaving aside the practical ineffectiveness of prohibiting personal use, there is a new complication on the horizon in the form of the "bring-your-own-device" ("BYOD") movement. BYOD means that the employer can no longer claim a proprietary interest in the device, which is usually stated as the basis for justifying the employer's right to control and monitor the use