PALLETT VALO LLP
Lawyers & Trade-Mark Agents

Your Authority For:
Business Law • Commercial Litigation • Commercial Real Estate
Construction • Insolvency & Corporate Restructuring
Labour & Employment • Wills, Estates & Trusts

www.pallettvalo.com

Privacy Law

November 2012

The Supreme Court of Canada continues to reshape and define the limits of privacy protection in the face of rapid technological change. In two recent decisions, the Court has upheld and acknowledged important privacy interests of both employees and victims of Internet bullying, but restricted the rights of Internet commentators to remain anonymous in cyberspace.

IT'S PERSONAL: EMPLOYEES HAVE PRIVACY RIGHTS IN WORK COMPUTERS

In its most recent privacy decision, *R. v. Cole*, 2012 SCC 54, the Supreme Court confirmed that employees may have a reasonable expectation of privacy with respect to the information stored on their work computers, even where an employer has computer use policies in place.

The accused in *R. v. Cole* was a high school teacher who had been issued a laptop by the school board for which he worked. The school's policies stated that all data stored on work-issued equipment remained the property of the board, but that employees were permitted to use school computers for incidental personal purposes. While doing system maintenance of Mr. Cole's laptop, a board technician discovered nude photographs of an underage female student, which Mr. Cole was alleged to have downloaded from a computer used by another student in the school's computer lab. The technician reported his findings to the school principal who turned the laptop over to the police.

In determining whether the pictures and other data found on the laptop were legally admissible as evidence to support criminal charges, the Court had to consider whether Mr. Cole's *Charter* rights were infringed when the laptop was given to the police without a search warrant. The *Charter* protects individuals against unreasonable search and seizure and requires improperly obtained evidence to be excluded if admitting that evidence would bring the administration of justice into disrepute.

A Reasonable Expectation of Privacy

In considering whether Mr. Cole's *Charter* rights were violated by the warrantless surrender, the Court had to determine whether he had a reasonable expectation of privacy with respect to the information stored on the laptop. The Court said that informational privacy is an important interest because it relates to our ability to determine for ourselves when, how and to what extent information about us is communicated to others. Any computer that is used for personal purposes contains details about the user's financial, medical and personal situation, and reveals the user's interests, likes and habits. The Court said that it was reasonable to think that this biographical information should be private.

The Court also considered whether the ownership of the computer and the context in which it was used reduced an employee's expectation of privacy. The Court noted that the employer's policies and workplace practices could, in some circumstances, reduce a reasonable employee's expectation of privacy. But the fact that employees were permitted to use their computers for incidental personal purposes meant that highly personal information could be stored on those computers. Therefore, notwithstanding the employer's policies, the employee did have a privacy interest in the laptop, and the surrender violated his *Charter* rights. In the final analysis, however, a majority of the Court found that the evidence was admissible on the facts of this case.

What it Means for Business

Although it was a criminal case, the Supreme Court's decision in *R. v. Cole* has some important implications for private sector employers. The Court's analysis indicates that employees can reasonably expect that personal information found on their work computers should remain private, even if the employer owns the equipment and has policies claiming ownership rights to electronic data. An employer's policies with respect to computer and network equipment may reduce an employee's expectation of privacy, but will not usually eliminate it.

This means that even private-sector employers (who are not subject to the *Charter*) should think twice before allowing the police and other regulatory bodies to search their computer equipment without a warrant if there is a possibility that the search may reveal employees' personal

information. While the tort of invasion of privacy is still very new in Ontario (see our February 2012 newsletter on *Jones v. Tsige* for more information), it is conceivable that an employee might seek legal recourse against an employer that intentionally or recklessly disclosed his or her personal information without consent.

The Court's decision in *R. v. Cole* also acknowledges that the line between personal and work-related use of connected devices – such as smart phones, tablets and laptops – has become increasingly blurred. As more and more work-related information is found in the Cloud or on social media sites liked LinkedIn and Twitter, the employer's ownership of the physical infrastructure has become much less important in evaluating privacy interests.

An employer's ability to assert ownership and control over computer equipment used by its employees will depend on the circumstances and the "operational realities" of the workplace environment. In some cases, it may be appropriate to review written policies and procedures restricting personal use of workplace computers and monitor employee compliance. This may help to reduce a reasonable employee's expectation that personal information found on work computers will remain private.

Attempting to restrict employees from all personal use of workplace computers is increasingly unrealistic and often counter-productive, however, so it is likely impossible to eliminate all employee privacy interests in electronic data. Employers seeking to monitor employees' personal Internet usage or personal email for legitimate business reasons may wish to seek legal advice before proceeding.

BULLIES UNMASKED: CYBERBULLYING DECISION MAY LIMIT ANONYMITY ON THE INTERNET

Another timely Supreme Court privacy decision, *A.B. v. Bragg Communications Inc.*, 2012 SCC 46, addresses the power of social media to destroy the reputation of a person or organization almost instantaneously. The case also acknowledges that the victims of social media abuse are often powerless to proceed without drawing even more negative attention to their plight. In a landmark case on cyberbullying, the Supreme Court of Canada recently allowed the15-year-old victim of a fake Facebook page to sue the page's author without disclosing her own identity.

The Trail of the Internet Bully

The fake Facebook page at issue in *A.B. v. Bragg Communications Inc.* contained a picture and slightly modified version of the name of the young woman, identified only as A.B., along with sexually explicit references and disparaging remarks about A.B.'s appearance.

Facebook disclosed the IP address and location of the computer that had created the fake Facebook account. The IP address led to the poster's Internet Service Provider (ISP), which agreed to provide more specific information about the poster's address, as long as it had authorization from the court to do so.

A.B., with her father as litigation guardian, then brought an application for a court order requiring the ISP to disclose the identity of the person or persons using the IP address so that the potential defendants in a defamation action could be identified. As part of her application, A.B. asked the court to conceal her identity during its proceedings and in its written judgments. She also asked for a publication ban to keep her real name and identity out of the media.

The Halifax Herald and Global Television appeared as interveners in the initial proceedings. They argued that the open court principle and freedom of the press should trump A.B.'s privacy interests, claiming that the use of initials in court proceedings makes the justice system inaccessible to the public.

Courts May Order Internet Posters Unmasked

At the initial hearing, the Nova Scotia Supreme Court first had to decide whether to grant the application to order the ISP to disclose the requested information. The Court referred to *Warman v. Wilkins-Fournier*, a recent Ontario decision in which the Divisional Court had stated that allowing someone to libel and destroy another person's reputation while hiding behind a cloak of anonymity was not in the public interest.

The Nova Scotia Supreme Court held that while commentators should be allowed to remain anonymous in

some cases (such as when expressing political dissent), in most cases posters should not expect to remain anonymous. An Internet poster's expectation of anonymity is not reasonable if there is an apparent case of defamation and no compelling public interest that supports the poster's desire to conceal his or her identity.

Privacy vs. Open Courts

The Nova Scotia trial court also had to consider whether A.B. should be identified only by her initials and whether a publication ban should be ordered over the court's proceedings. In denying the publication ban, the Nova Scotia court relied on a case in which the Supreme Court of Canada held that a publication ban should only be ordered when it was needed to protect the proper administration of justice and the need for the ban outweighed other interests such as the right to free expression and the right of the accused to a fair and public trial.

The trial court found that was no evidence that A.B. would suffer any additional harm if information about the case was made public or if her real name was used in court proceedings and held that a publication ban was not justified.

A.B. then appealed the trial court's decision to deny the publication ban and prevent her from proceeding without using her real name. The Nova Scotia Court of Appeal upheld the trial decision, finding that our legal system starts with the presumption that courts will be open to the public. The Court of Appeal found that A.B. had failed to lead any evidence that she would be harmed by having to reveal her identity and denied the publication ban.

Supreme Court's Balancing Act

Demonstrating that the fake Facebook author had definitely picked on the wrong victim, A.B. appealed the Nova Scotia Court of Appeal's decision to the Supreme Court of Canada where she was largely successful.

Many interest groups intervened on A.B.'s behalf, leading evidence suggesting that allowing the names of bullying victims to be made public can exacerbate their trauma. The Supreme Court agreed, recognizing the harm that bullying causes children and the importance of preventing it.

The Court held unanimously that A.B. should be entitled to proceed anonymously, but limited the publication ban to only allow publication of the non-identifying content of the fake Facebook profile once A.B.'s real identity had been protected. The Court also noted that the partial publication ban protecting A.B.'s real name would have only a minor effect on the news media as they would still be able to report on the case.

What it Means for Business

Publication bans and anonymous proceedings are most commonly used in criminal and family law decisions but are rarely sought in civil disputes. In exceptional circumstances, however, a court may make a sealing order during civil proceedings to protect trade secrets or other commercially sensitive information.

A.B. v. Bragg Communications Inc. is a rare example of a case in which publication has been restricted in the civil litigation context. While the Supreme Court's decision to favour the plaintiff's privacy interests over the open court principle may have been largely based on its concern for the vulnerability of children and youth, the decision effectively expands the court's power to protect the privacy of parties to litigation.

Business owners will also take comfort in the fact that all three levels of court upheld the right of the subject of an allegedly defamatory Internet posting to seek information from the ISP about the poster's identity based on the IP address. Although this is not a new development, it is good news for businesses that have had their reputation unfairly tarnished online.

To obtain the identity of anonymous Internet posters, the courts have held that plaintiffs will first have to make out a *prima facie* case of defamation. This can be done by showing that (1) the anonymous posting was defamatory in the sense that it would tend to lower the plaintiff's reputation in the eyes of a reasonable person; (2) the posting actually referred to the plaintiff rather than to somebody else; and (3) that the words in the posting were actually published, meaning that they were communicated to at least one person other than the plaintiff.

Second, the plaintiff will have to show that there is no a compelling interest that would favour anonymity, such as the need to protect freedom of speech and political commentary. A business that is the subject of an anonymous Internet posting may be able to obtain the information needed to pursue a cause of action if they can show that these two conditions have been met.

A.B. v. Bragg Communications also serves as a reminder that nothing posted online is truly anonymous and there are remedies available if defamatory comments are made online.

The authors would like to thank Steven Pordage, Student-at-Law, for his assistance in preparing this bulletin.

Pallett Valo LLP Privacy Law Group

Pallett Valo LLP's Privacy Law Group advises and supports private sector organizations to comply with their obligations under the *Personal Information Protection and Electronic Documents Act*. We assist our clients in developing privacy policies and practices to meet strategic business needs and to ensure compliance with privacy legislation. We are also experienced in advising clients regarding the *Freedom of Information Act and Protection of Privacy Act* and the *Municipal Freedom of Information and Protection of Privacy Act*.

Contact Members of the Privacy Law Group

Greg Azeff gazeff@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 264

Andy Balaura abalaura@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 225

Joe Conte jconte@pallettvalo.com
Direct Dial: 905.273.3022 Ext. 217

Greg Azeff is a member of the Privacy Law Group.

Andy Balaura is a member of the Privacy Law Group.

Joe Conte is a member of the Privacy Law Group.

This article provides information of a general nature only and should not be relied upon as professional advice in any particular context. For more information about Privacy Law, contact a member of our **Privacy Law Group** at **905.273.3300**.

If you would prefer to receive your bulletins by email, visit www.pallettvalo.com/signup or send an email to marketing@pallettvalo.com.