l'Association canadienne du droit
des technologies de l'information

October 21, 2010

IT.Can NEWSLETTER

Canadian IT Law Association

www.it-can.ca

This newsletter is prepared by Professors Robert Currie, Chidi Oguamanam and Stephen Coughlan of the Law and Technology Institute of Dalhousie Law School.

Les auteurs du présent bulletin sont les professeurs Robert Currie, Chidi Oguamanam et Stephen Coughlan de l'Institut de droit et de technologie de la Faculté de droit de l'Université de Dalhousie.

No Discretion to Exclude: Business Method is Patentable in Canada!

The Federal Court in Ottawa, ON, has delivered its decision in *Amazon.Com, Inc. v. the Attorney General of Canada,* and the Commissioner of Patents. The case involves the appellant's patent for an invention entitled *Method and System for Placing a Purchase Order via a Communication Network* (a.k.a. one-click ordering system). Simply expressed, under this invention, a customer visits a website and enters their address and payment information and obtains an identifier which is stored in a cookie in their computer. The enabling server is then able to recognize the customer via their computer with the identifying cookie and then recalls the purchasing information which is stored in the appellant vendor's computer to enable the customer purchase an item by way of only a single click without checkout requirement and without supplying additional information. The patent application was denied by the Commissioner of Patents on a number of grounds, notably (for the present purpose) that it is a business method patent which, according to the Commissioner, was not patentable subject matter under s.2 of the *Patent Act*.

In making her finding, the Commissioner relied on a four-step approach of assessing patentability of an invention. That approach involved extensive analysis around the form and substance of the applicant's claims, the definition of relevant categories of invention, especially in regard to whether the invention in question constituted an art, an analysis of excluded subject matter under the *Patent Act* and an inquiry regarding the technological requirement of the invention. The Federal Court faulted the Commissioner's approach and findings in regard to the four steps, declaring them to be inconsistent with the law in Canada. Specifically, the court denied that there is technological requirement or a "technical test" recognized under the *Patent Act* in assessing the patentability of an invention and noted that "[i]t is not within the Commissioner's jurisdiction to introduce one" (¶70). The Court held that in arriving at her conclusion that the appellant's invention involved non-patentable subject matter, the Commissioner relied excessively and wrongly on international legal principles to interpret the Canadian patent regime. Specifically, reliance on UK and Europe is not helpful because under those systems there is no definition of invention, but the interpretation of invention is a negative exercise to determine whether what is claimed should be classified as excluded subject matter under Article 52 of the *European Patent Convention*. That is not the approach in Canada, US and even Australia where there is clear statutory attempt to define invention. According to the Federal Court, the Commissioner was flatly wrong to hold that business method patent is excluded under the Canadian patent regime. In Canada, inventions are defined by the claims and ought to be interpreted in a purposive manner. The Commissioner of Patents in Canada has no discretion pursuant to the *Patent Act* to refuse any patent on the basis of imaginary exclusion or public policy.

The court held that: "There is not, nor has there ever been, a statutory exclusion for business methods in Canada as there is in the UK" (¶63). Fundamental principles for exclusion of invention from patentability ought to apply to business methods as they apply to all other inventions. In this regard, mere business schemes or methods which have no practical embodiment like any theorem or abstract idea are not patentable. The appellant's invention or claims in this case have practical embodiment and are perfectly patentable under the *Patent Act.* In upholding the appeal, the court held that, for the most part, as it is in the United States and Austria,

so it is in Canada: We allow "business methods to be assessed pursuant to general categories in s. 2 of the *Patent Act*, preserving the rarity of exception ... avoid[ing] the difficulties in the UK and Europe in attempting to define a "business methods"... Contrary to what the Commissioner suggests, to implement a business method exception would be a radical departure from the current regime requiring parliamentary intervention" (¶68).

Google Breached PIPEDA: Privacy Commissioner

The Privacy Commissioner of Canada, Jennifer Stoddart, has concluded an investigation into Google by determining that the company violated the *Personal Information Protection and Electronic Documents Act (PIPEDA)*. In her Preliminary Letter of Findings, the Commissioner outlined how her office initiated the investigation in May 2010 after it came to light (in part via voluntary disclosures by Google) that Google's street view cars had inadvertently collected personal information from unsecured wireless networks as part of WiFi monitoring projects. The information included "substantial amounts of personal information in the form of e-mail message content (e.g., e mail, IP and postal addresses)," as well as a list of names of people who were suffering from certain medical conditions. Given that consent had not been sought or given the collection Google had seriously breached Principles 4.2, 4.3 and 4.4 of the Act. The collection occurred via software which had been developed by a Google engineer but not submitted for review by Google's product counsel, a "careless error," the negative effects of which could have been "easily avoided." She also found that the code in question had not been sufficiently tested for privacy impact.

However, upon discovering the error Google had grounded its vehicles and isolated the data which had been collected, and committed to protecting it until it was deleted. Accordingly, the Commissioner found that Google had upheld the safeguard provisions of the Act. Her recommendations included increasing the scope of privacy training for employees, putting in place a governance model that would ensure screening procedures were followed prior to the release or use of a new product, and the deletion of the data. Google has until 1 February 2011 to implement the Privacy Commissioner's recommendations.

When CSIS Strays into Criminal Investigation: Duty to Comply with the *Charter*

The Ontario Superior Court has delivered its ruling in an application by the accused in *R. v. Mejid* (hyperlink not available, digest here) for an order excluding evidence of child pornography found in the accused's computer pursuant to s. 24(2) of the *Charter*. The accused argued that the seizure of the computer in question by officers of the Canadian Security Intelligence Service (CSIS) breached his s.8 *Charter* rights. The accused has been a person of interest to the CSIS since at least 2003. CSIS officials have suspected the accused of having some association with terrorist organizations, including Al Qaeda and a number of other Islamic extremist movements. They also alleged that he was actively involved with posting terrorist-related literature in various websites and operated under some other pseudonyms. Since 2003, a number of CSIS officials maintained contact with the accused, inviting him for interrogation on several occasions whereof they restated their numerous accusations against him. On evidence, most the officers were of general impression that that the accused was mainly cooperative through these encounters. They claim that he voluntarily allowed them access to his computers which CSIS agents took possession of, often for days. According to the accused, he relinquished his computers essentially as a result of the pressures and threats posed by those agents and his inclination to clear his name and to prevent CSIS agents from executing a warrant of search on his residence which they have threatened. The accused feared that executing such a warrant would put him and his family in an embarrassing situation with his community.

On October 12, 2007 the accused mistakenly strayed into the United States while driving. He was then stopped and detained at the border as he did not have relevant documents to re-enter Canada. While detaining the accused, the Canada Border Services Agency (CBSA) alerted CSIS which despatched an officer familiar with the accused's case to the

border. There again, the accused was subjected to interrogation on national security matters. He produced his laptop computer to CBSA official who searched it on the advice of the CSIS agent, but given the CBSA personnel's limited knowledge she did not do a thorough search of the computer, which was then returned to the accused. Four days later, the accused met with CSIS agents for continued interrogation in a hotel room at CSIS' invitation. Under pressure and threat, he gave his laptop computer to the agents who not only copied its hard drive but also did a comprehensive analysis of the computer, reviewing every file without informing the accused. The analysis of the hard drive revealed images of child pornography for which the accused was charged with 2 counts of possessing child pornography and one count of accessing, making and distributing child pornography.

In allowing the application, the court held that the CSIS agents' role turned from that of collecting intelligence regarding national security to a criminal investigation on October 12, 2007. The court observed that "[t]he investigation of criminal matter falls outside the mandate of CSIS" (¶84). At the point CSIS' interest turned to investigation of criminal activity, the police should have been called and the accused should have been advised that the police could use any materials recovered from him for subsequent prosecution of his alleged crime. The accused did not understand the implication of this and no one explained it to him. The court found that the accused did not provide his consent in regard to CSIS access to his computers; he rather acquiesced to the demand and pressures of the CSIS agents. According to the court, acquiescence should not be conflated with cooperation or compliance with police requests. That the accused could not object to the conduct of CSIS agents in accessing his computer did not mean he consented because he acted under state intimidation, pressure and coercion. His decisions in the circumstances were neither voluntary nor informed. The seizure of his computers in regard to criminal investigation was not done in compliance with s. 8 of the *Charter* and to admit such evidence would bring the administration of justice into disrepute. It was in the interest of justice to distance the justice system from a process that evidently demonstrated a flagrant breach of the accused's *Charter* rights.

Student Facebook Posts Protected by *Charter*

In *Pridgen v. University of Calgary*, Justice J. Strekaf of the Alberta Court of Queen's Bench sat in judicial review of a disciplinary decision by the University of Calgary's General Faculties Council Review Committee (the "Committee"). Two students, Keith and Steven Pridgen, were undergraduate students in a course taught by an unpopular professor, and each posted critical comments about the professor on a Facebook page. The professor reported the postings to the Dean of the Faculty of Communication and Culture, who held that each of the students had committed non-academic misconduct and levied various administrative penalties. On review, the Dean's finding of misconduct was upheld by the Committee, which revised the penalties to a period of academic probation for each student. The students sought judicial review, arguing that the actions taken by the University infringed their rights to freedom of expression and freedom of association in contravention of sections 2(b) and 2(d) the *Charter*.

Strekaf J. began by reviewing the Supreme Court of Canada's jurisprudence on whether and when universities and similar public institutions are subject to *Charter* scrutiny, concluding in part that "the *Charter* may apply in one of two ways; it may apply to a government actor or it may apply to non government actors responsible for the implementation of a specific government policy or activity" (para. 48). Reviewing the legislative scheme by which the University had been created, she concluded that, similarly to the Supreme Court of Canada's finding in *McKinney v. University of Guelph*, the University was not a government actor. However, pursuant to the University's founding statute, she held that it was "acting as the agent of the provincial government in providing accessible post secondary education services to students in Alberta" (para. 59). This was because the University was "tasked with implementing a specific government policy for the provision of accessible post secondary education to the public in Alberta" (para. 63). The disciplinary powers in question were part of this function and were thus subject to the *Charter*:

> When a university committee renders decisions which may impact, curtail or prevent participation in the post secondary system or which would prevent the opportunity to participate in learning opportunities, it directly impacts the stated policy of providing an accessible educational system as entrusted to it under the *PSL Act*. The nature of these activities attracts *Charter* scrutiny (para. 67).

Applying the Supreme Court of Canada's jurisprudence on section 2(b)'s protection of freedom of expression (the court held that section 2(d) had not been infringed), Justice Strekaf held that i) the posts in question had expressive content and conveyed meaning; and ii) the purpose of the Committee's order had been to restrict the students' freedom of expression. Accordingly, section 2(b) had been infringed. She further ruled that the breach could not be saved under section 1 of the *Charter* because the orders did not impair the rights as little as possible, stating: "Students should not be prevented from expressing critical opinions regarding the subject matter or quality of the teaching they are receiving… While certain of the comments made about Professor Mitra were not particularly gracious and might have reflected a lack of maturity, the Facebook Wall does have utility as a forum of discussion. The commentary may assist future students in course selection as well as provide feedback to existing students and perhaps reassurance that one is not alone in finding that they are having difficulty appreciating instruction in a particular course" (para. 82).

The court also found that the University had denied the students procedural fairness because the reasons for the decisions were inadequate, and that there was no reasonable basis for the conclusion that the statements had constituted non-academic misconduct because there was no evidence of injury to the professor. Accordingly, the decision of the Committee were quashed.

E-Disclosure: Attachment is Part of E-mail for Discovery Purposes

In *Guestlogix v. Hayter*, the plaintiff's affiant (Proud) had refused to answer some questions and produce documents when he was discovered. The defendants made a motion to compel answers to the questions and production of the documents. One of the documents in question was an attachment to an e-mail which had previously been produced. The plaintiff argued that the attachment itself was not relevant to the subject matter of the overall action. The motions judge, D.M. Brown J., rejected the argument and ruled as follows (at para. 21):

> I need not consider the issue of relevancy for this question. The document sought was an attachment to an email that was produced and marked as an exhibit on Mr. Proud's cross-examination. An email and any attachments constitute an integrated communication. Both the email text and the attached text, in whatever format, are discrete elements combining to form one integrated electronic communication. If one part of the communication is produced, the remainder must be produced as well in the absence of any assertion of privilege, of which, in this case there is none. Accordingly, if a party produces the text of an email, it must also produce any attachments to that email.

CBC News: Dangers of Transferring Digital Data Storage Device

Who has the obligation to rid a data storage device of captured data, especially when the data in question involves personal information, before such a device is disposed of? What are the privacy and legal implications of a failure to discharge any such obligation? At what point or in what circumstance does the obligation to destroy digital data become an ethical obligation? What is a fool-proof way of destroying unwanted digital data? Would that necessarily involve the destruction of the digital storage device itself? Does the nature of digital data capturing device (e.g. laptop, ipad, iphone, blackberry, regular cell phone, digital camera, digital fax and copiers (with memory/storage capacity)) etc. matter? Recently, these and related question are matters of interest in the blogosphere and at the Bar. The Florida State Bar, for example, recently released a proposed advisory opinion that lawyers have "an affirmative obligation" to maintain their competence

in media-based technology and to ensure that any information storage media which contain confidential client information have been "scrubbed" prior to disposal.

A recent investigative report by the CBC News: "Copy Machines Spill Identity Secrets" revealed an alarming discovery underscoring the urgency of the above questions. The CBC bought a used photocopier from a UPS franchise via kijiji's online classified advert. The copier's two hard drives were run through a laptop computer and it was discovered that the units were not rid of captured data before they were resold. According to the CBC report, further forensic assessment and analysis of the drives revealed over 100 documents on one of the hard drives, which included income tax returns, health information, driver's licence, citizenship card and various business documents.