

McCarthy Tétrault Co-Counsel:
Technology Law Quarterly

Volume 3, Issue 2
April - June 2007



The right people. The right results.®

McCarthy
Tétrault

Co-Counsel:

Technology Law Quarterly

Volume 3, Issue 2

Welcome to Volume 3, Issue 2 of *McCarthy Tétrault Co-Counsel: Technology Law Quarterly*. In this issue of the TLQ, we highlight some new developments in tech law and, for the first time, introduce a new section dedicated to clean technology initiatives. On the Internet side, new and emerging websites involving virtual worlds, like Second Life and Weblo, are hot commodities. These 3-D Internet-based virtual societies created entirely by their residents offer opportunities to make virtual friendships, purchase virtual properties and develop virtual social and business relationships. Our article on this topic speaks to the rights and obligations that arise between the creator of a virtual world and its residents. On the electronic records retention front, our lawyers have summarized and analyzed some important amendments to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* that impact record-keeping requirements and verification of identity of suspicious transactions.

On the intellectual property front, two key areas are discussed. In the copyright world, online search engines and their ability to play a critical role in curbing access to infringing copyright material is discussed in light of a recent and important US case. On the patents side, a ruling in the *KSR* case on the law of obviousness in patents in the US was handed down and our lawyers explain the impact for our patent clients.

Privacy continues to be a hot topic, and we've included four interesting pieces in the area. The first addresses a Parliamentary committee's recommended amendments to *PIPEDA* after extensive consultations with several stakeholders. The second takes an in-depth look at privacy breaches and computer security, particularly the surge in breaches as a result of the Internet and newer forms of related technologies. In an article that mixes privacy with power and electricity, our lawyers examine new cutting-edge technology behind the US-based concept of Demand Response, which lowers energy costs while increasing electricity consumption – but also raises important privacy concerns. The last article deals with a court's analysis on the disclosure of personal information without consent pursuant to a lawful authority exception for gathering intelligence.

Lawyers from our communications practice group were at the forefront of drafting an Act whose legislative provisions implement key recommendations of the Telecommunications Policy Review Panel's 2006 report. As well, we continue our four-part discussion on regulatory issues affecting VOIP technology with a detailed overview of some recent CRTC decisions.

On the biotech side, this edition of the TLQ examines an interesting dichotomy between the academic and corporate worlds when understanding the process of renegotiating university biotechnology licenses. The clash of culture between the need to advance scientific knowledge sharing and publishing of data versus maintaining market value through exclusive rights to generate maximum profits is a challenging one.

The right people. The right results.®

McCarthy
Tétrault

Lastly, we introduce a new section to the TLQ entitled Clean Technology where we share our experience on 'cleaner,' knowledge-based technologies designed to improve functional operations, productivity and efficiency while reducing corporate costs. In this issue, we discuss venture capital investment in the clean tech space.

These and many other key topics are discussed in this issue of the TLQ. Browse through the publication using the table of contents, which contains 'clickable' links to articles. As well, all the articles can be found on our website [here](#). You can search our publications database and find additional informative articles on many subjects. If you would prefer to receive a paper copy of the TLQ in the future or wish to change your subscription information, please contact me at the link below.

McCarthy Tétrault is proud of its position as a leader in all areas of law. The *Canadian Legal Expert Directory 2007* has recognized McCarthy Tétrault for having the premier technology law practice in the country. The *Chambers Global: Guide to the World's Top Lawyers 2007* has confirmed McCarthy Tétrault's top ranking in Canada for technology, media and telecom (TMT). *Co-Counsel: Technology Law Quarterly* is one more way we are working hard to retain that position of leadership.

[Sukesh Kamra](#)
Editor-in-chief
July 2007

McCarthy
Tétrault

Table of Contents

Internet/E-World	1
E-COMMERCE	1
<u>International</u> : Second Life – Virtual Property Rights and Obligations	1
<u>New York</u> : Intangible Property and the Law of Conversion	2
SOFTWARE LICENSING	3
<u>International</u> : FSF Releases Version 3 of GNU GPL	3
RECORDS RETENTION	6
<u>Canada</u> : Important Amendments to the <i>Proceeds of Crime (Money Laundering) and Terrorist Financing Act</i> come into Force	6
Intellectual Property	9
COPYRIGHT	9
<u>U.S.</u> : Online Search Engines and Copyright Infringement	9
<u>Europe</u> : Significant Win for Music Industry versus ISPs	10
TRADE-MARKS	11
<u>U.S.</u> : Utah Legislation for ‘Electronic Registration Marks’ Delayed	11
PATENTS	14
<u>U.S.</u> : Supreme Court Hands Down <i>KSR</i> Ruling	14
Privacy	16
CASES/LEGAL DEVELOPMENTS	16
<u>Canada</u> : Committee Recommends Amendments to Canada’s Federal Privacy Legislation	16
<u>Canada</u> : Disclosure of Personal Information without Consent Pursuant to Lawful Authority	18
<u>Canada</u> : Computers and the Emergence of Privacy Breaches	20
<u>Canada</u> : New Electricity Technologies and Their Privacy Implications	23

Communications	27
CASES/LEGAL DEVELOPMENTS	27
<u>Canada</u> : Model Act to Implement Telecom Sector Reform Released	27
<u>Canada</u> : Voice over IP Services – Regulatory Perspectives from the Developed and Developing Worlds – Part II.....	27
 Biotechnology/ Life Sciences	 34
CASES/LEGAL DEVELOPMENTS	34
<u>Canada</u> : Renegotiating University Biotechnology Licenses.....	34
 Clean Technology	 38
CASES/LEGAL DEVELOPMENTS	38
<u>Canada</u> : Clean Technology Coming of Age.....	38

Internet/E-World

E-COMMERCE

International: Second Life – Virtual Property Rights and Obligations

Virtual-world role-playing games are fast becoming a routine activity for millions of people around the world. Operators of virtual-world websites allow users to create avatars to represent themselves and interact with other avatars limited only by human imagination. Many people live large portions of their lives forming virtual friendships, building and acquiring virtual properties, and forming social and business organizations and relationships.

McCarthy Tétrault Notes:

In a recent case before a court in Pennsylvania, a plaintiff claimed an ownership interest in a virtual property that he purchased with real money. The plaintiff contends that the operators of the website unlawfully confiscated his property and froze his virtual currency account.

The defendants operate the popular virtual world known as Second Life. The defendant has recognized that all participants acquire an intellectual property interest in the digital content they create or otherwise own. This fact distinguishes Second Life from most other virtual worlds.

The issue before the courts is what rights and obligations grow from a relationship between the owner and creator of a virtual

world and its resident customers. According to the defendant, the property the plaintiff claims he purchased has been unlawfully acquired. In addition to this issue above, the courts tackled two other fundamental issues – jurisdiction and the enforceability of the arbitration provision found on the website’s terms of use.

The court held that the defendant had minimal contacts with the state of Pennsylvania to support specific personal jurisdiction since the plaintiff established that the defendant induced people to purchase virtual land and property on Second Life. The defendant also made representations in the US targeting all states and not specifically one state. Furthermore, the defendant took a personal role in generating additional traffic to the website by enticing customers to enter. In other words, the court held that the site’s marketing efforts were more interactive than merely passive.

On the issue of compelling arbitration, the court held that users must accept the terms of service of Second Life. The terms of service contain a provision that requires mandatory binding arbitration in the city of San Francisco. The *Federal Arbitration Act* requires that the court apply federal substantive law in this case because the arbitration agreement is connected to a transaction involving interstate commerce. The plaintiff argues that the terms of

service's arbitration provision is unconscionable because it deprives him from his day in court. The law requires the court to apply California state law to determine the enforceability of the arbitration provision. To find unconscionability, the procedural component can be satisfied by proving oppression through the existence of unequal bargaining power or surprise through hidden terms common in the context of adhesion contracts. The substantive component can be satisfied by showing overly harsh or one-sided results that shock the conscience.

The court held that the terms of service are clearly part of a contract of adhesion and the defendant has superior bargaining strength. In addition, the arbitration provision is buried in a rather lengthy paragraph under the benign heading 'general provisions.' Failure to make available the costs and rules of arbitration in the terms of service adds to this situation. The court also took an in-depth look at the substantive element of the provision and held that the provision lacked mutuality, in that the terms of service provide the defendant with a variety of one-sided remedies to resolve disputes and force the participant to arbitrate disputes. In fact, the costs of proceeding through arbitration far exceed litigation through state or federal court, and the venue is restricted to the defendant's place of business. Finally, the defendant, under the terms of service, may

unilaterally decide to freeze a participant's account, refuse access to virtual and real currency and confiscate the participant's virtual property. A participant must then, if he so desires, initiate arbitration only in the defendant's place of business.

Given the facts above, the court found the arbitration provision unconscionable and refused to enforce it. It also held that it could not cure the contractual deficiency by severing or restricting the clause and was forced to void the entire agreement.

Contact [George S. Takach](mailto:gtakach@mccarthy.ca) in Toronto at gtakach@mccarthy.ca

New York: **Intangible Property and the Law of Conversion**

This case is an intriguing one that examines the long-standing discussion of paper versus electronic records. Several states have amended their respective legislation to recognize electronic records as having the same weight at law as paper ones. In this particular case, the plaintiff was an agent for the defendant and the defendant provided the plaintiff with a computer to carry out his functions. The plaintiff stored not only work-related documents on the computer but also personal documents and e-mail. Each night, the defendant uploaded information entered that day by the plaintiff to its own system. At some point, the defendant terminated his business relationship with the plaintiff and took possession of the computer. The plaintiff was

denied access to his personal documents and e-mail. He sued the defendant in conversion.

McCarthy Tétrault Notes:

The issue for the court was whether intangible property could be the subject of a claim in conversion. The court noted that traditionally this tort could only be successfully asserted in respect of tangible property, but it also noted that courts in some recent cases have extended the tort to intangible property. The court held that the tort should be available where intangible property is 'converted.' It viewed that the tort of conversion must keep pace with the realities of widespread computer use. It answered the certified question in the affirmative and held that the type of data that the defendant allegedly took possession of – electronic records that were stored on a computer and were indistinguishable from printed documents – are subject to a claim of conversion in New York. Otherwise, the law would give rise to anomalous results where, for instance, a difference would lie between setting ablaze a company's file room versus hacking into its computer system and deleting data.

Contact [Eric Gertner](mailto:egertner@mccarthy.ca) in Toronto at egertner@mccarthy.ca

SOFTWARE LICENSING

International: FSF Releases Version 3 of GNU GPL

On June 29, 2007, the Free Software Foundation released the long-awaited third version of the GNU General Public License (GPLv3). The GPLv3 is the culmination of an 18-month process, during which four drafts were prepared and made available for public review and comment. It marks the first update since 1991 to what the Free Software Foundation calls "the world's most popular free software license."

McCarthy Tétrault Notes:

The GPL: A Brief Overview

The GNU General Public License is the most popular form of 'copyleft' free software license. According to Richard Stallman, the founder and president of the Free Software Foundation and original author of the GPL, the purpose of the GPL is "to guarantee every user the freedom to run, study, adapt, improve and redistribute" the software licensed under it. The core rule governing the GPL is that anyone is free to use, copy, modify and distribute software licensed under the GPL, as long as any distribution of that software, or of any software that is derived from GPL-licensed software, is also distributed under the GPL, with the source code made available to the public. Many of the most significant open source programs, including the Linux operating system, are distributed under the

GPL. However, companies that wish to derive value from the development of proprietary software products generally avoid GPL software so that the GPL software does not 'taint' the proprietary software and possibly render the resulting combination subject to the requirements of the GPL.

The most recent version of the GPL has been a long time in coming. The Free Software Foundation has described the changes that it made as necessary "to deal with the new threats to free software that have emerged since version 2 of the GPL," as well as to provide certain important clarifications and improvements to version 2. The most significant changes are described below.

Key Changes in Version 3

The most significant changes incorporated into the GPLv3 are the following:

1. *Digital rights management (DRM)* – Some countries have enacted laws (such as the *Digital Millennium Copyright Act* in the U.S.) that prohibit the intentional circumvention of technological measures designed to prevent illegal access to or copying of a copyrighted work. Such technologies, known as DRM technologies, are used increasingly to protect digital content such as music, videos and games. The GPLv3 provides that anyone distributing software under it must "waive any legal power to forbid circumvention of

technological measures" relating to such software. In other words, anyone distributing software under the GPLv3 must waive any potential claim that it may have under anti-circumvention laws.

2. *Prohibition on 'tivoization'* – 'Tivoization' was coined to describe a practice in which a system that includes open source software uses hardware to prevent the modification of the open source software. The term arose when TiVo drew the ire of the open source community because its devices, which ran a number of GPL applications, would cease to operate when modifications were made to the internal software. The GPLv3 expressly forbids 'tivoization' by requiring any GPL software distributed as part of a consumer product to include installation information sufficient to enable modification of the GPL software, and to ensure that modifications do not prevent or interfere with the continued functioning of the code.
3. *Patent licenses* – Version 2 of the GPL did not contain an express patent license, though arguments were made by several stakeholders that a patent license should be implied from its terms. The GPLv3 now includes a grant of a non-exclusive, worldwide, royalty-free patent license under the licensor's "essential patent claims" (which is

broadly defined as “all patent claims owned or controlled by the contributor, whether already acquired or hereafter acquired, that would be infringed by some manner, permitted by this License, of making, using or selling its contributor version”). The GPLv3 also prohibits distribution of GPL software by anyone who has acquired a “discriminatory” patent license in respect of such software that would be available, for example, to its own customers, but not to others. This prohibition was included specifically in response to the settlement reached between Microsoft and Novell in 2006, pursuant to which Microsoft agreed not to assert patents against customers using Novell’s Linux product in return for payments from Novell. It is designed to prevent future entry into such arrangements.

4. *Termination cure period* – Under the previous version of the GPL, any violation resulted in automatic termination of the license. The GPLv3 makes some progress towards aligning itself with standard licensing terms, by giving first-time violators a 30-day cure period to remedy the violation.

Is it an Improvement?

The question of whether or not the GPLv3 is an improvement over its predecessor has already sparked a great deal of debate. Not surprisingly, those in favour of intellectual property rights protections and controls are

less than enthusiastic. This faction has predicted that the GPLv3 will create a larger chasm between open source and proprietary software, making it more difficult and risky to freely integrate them. Others have expressed concern over the unclear and overreaching language in some of the new additions, with particular concern expressed over the new terms relating to patents. Interestingly, even some open source software supporters, including Linus Torvalds, the developer of the Linux kernel, have indicated that they do not support this new version, and have specifically decried the new section relating to DRM. Proponents of the GPLv3, on the other hand, are celebrating a positive step forward in the Free Software Foundation’s “long history of fighting all efforts to make free software proprietary.” Time will tell whether the GPLv3 becomes a widely embraced standard for open source software.

Contact [Wendy Gross](mailto:wgross@mccarthy.ca) in Toronto at wgross@mccarthy.ca

RECORDS RETENTION

Canada:

Important Amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act come into Force

Amendments that Came into Force on June 30, 2007

A number of important amendments found in Bill C-25, *An Act to amend the Proceeds of Crime (Money Laundering) and Terrorist Financing Act* came into force on June 30, 2007. The amendments enhance the identity verification requirements of financial entities that enter into a “correspondent banking relationship” with prescribed foreign entities and expand the scope of allowable disclosure of “designated information” by Financial Transactions and Reports Analysis Centre of Canada (FINTRAC).

McCarthy Tétrault Notes:

Correspondent Banking

One of the important amendments that came into force on June 30, 2007 requires certain entities to take specific cautionary measures before entering into a “correspondent banking relationship” with a prescribed foreign entity. “Correspondent banking relationship” is defined in the amended section as a relationship created by an agreement under which one of the specified entities undertakes to provide a prescribed foreign entity with financial

services, such as international electronic fund transfers, cash management and cheque clearing. The amendment also prohibits any person or entity from entering into a “correspondent banking relationship” with a shell bank.

Disclosure of Designated Information

The definition of “designated information” was expanded by the amendments that came into force on June 30, 2007 to include “attempted” financial transactions. This is consistent with a general expansion of the “designated information” FINTRAC may disclose in order to enhance Canada’s anti-money laundering and anti-terrorist financing regime. The amendments provide for additional disclosure to law enforcement and security agencies, as well as agencies such as Canada Revenue Agency and Canada Border Services Agency.

Amendments Coming into Force on June 23, 2008

A number of other important amendments to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) will not come into force until June 23, 2008. These amendments will expand the scope of record-keeping, reporting and registration requirements, with the intention of enhancing Canada’s anti-money laundering and anti-terrorist financing regime.

Record-Keeping

As of June 23, 2008, the PCMLTFA's record-keeping regime will apply to persons and entities authorized under provincial legislation to engage in the business of dealing in any type of financial instrument and not simply those dealing in securities, as it does now. Furthermore, the application of the regime to foreign exchange dealing will extend to all persons remitting or transmitting funds by any means and those issuing or redeeming money orders, traveller's cheques or other similar instruments.

Attempted Suspicious Transactions

As discussed in the McCarthy Tétrault October 2006 newsletter, [Federal Government Introduces Amendments to the Anti-Money Laundering/Terrorist Financing Legislation](#), reporting entities will be required to report any attempted suspicious transaction to FINTRAC, as well as those actually completed. The amendments that will come into force on June 23, 2008 will also expand the scope of the reporting requirements to include persons or entities required to make a disclosure under the *Regulations Implementing the United Nations Resolutions on the Suppression of Terrorism*.

Identity Verification

A significant aspect of the amendments that will come into force on June 23, 2008 is the enhancement of client identification

requirements. No person or entity subject to the PCMLTFA shall open an account for a client without establishing their identity and determining whether the potential client is a "politically exposed foreign person." If a potential client does fall within the definition of "politically exposed foreign person," senior management approval is required before an account can be opened.

For additional information about the definition of "politically exposed foreign person," please refer to the McCarthy Tétrault October 2006 newsletter, [Federal Government Introduces Amendments to the Anti-Money Laundering/Terrorist Financing Legislation](#).

Registration

In order to enhance FINTRAC's ability to enforce the legislation, the amendments coming into force on June 23, 2008 will institute a federal registration system, under which individuals and entities falling into the categories of money services businesses and foreign exchanges businesses must register with FINTRAC. The amendment will also establish which persons or entities are not eligible for registration and will provide for a system of review, under which an entity can apply for a review of any decision to deny their application or revoke their registration. The review of any application, to be completed by the Director of FINTRAC, may be appealed to the Federal Court.

Regulations Amending Certain
Regulations Made Under the *Proceeds
of Crime (Money Laundering) and
Terrorist Financing Act*

On June 30, 2007, several provisions amending certain regulations made under the PCMLTFA came into force. These provisions include amendments to the definitions of “electronic fund transfer,” “financial entity,” “correspondent banking relationship” and “physical presence,” as well as a number of provisions that deal with enhanced reporting requirements relating to “attempted transactions.” Furthermore, the amended regulations now require enhanced identification and record-keeping requirements of financial entities entering into correspondent banking relationships with foreign financial institutions. Most of the new provisions amending the regulations made under the PCMLTFA, however, will not come into force until June 23, 2008.

Contact [Nancy Carroll](mailto:ncarroll@mccarthy.ca) in Toronto at ncarroll@mccarthy.ca

Contact [Barbara Mclsaac](mailto:bmcsaac@mccarthy.ca) in Ottawa at bmcsaac@mccarthy.ca

Contact Chris Hutchison in Ottawa at chutchison@mccarthy.ca

Intellectual Property

COPYRIGHT

U.S.: Online Search Engines and Copyright Infringement

The issue of online search engines and their ability to play a critical role in stopping access to infringing copyright material has been a very important one for rights holders.

McCarthy Tétrault Notes:

In this particular dispute between Perfect 10, a website featuring high-resolution photographs of topless or nude women, and Google, Perfect 10 notified Google that its thumbnail images and in-line linking to full-size images infringe Perfect 10's copyright. In particular, it alleges that the Google search engine program infringes its display and distribution rights. The court conducted an extensive examination of the factors needed to prove both infringing rights and held that Perfect 10 had a case against Google's thumbnail images, but it was still required to show a likelihood of success against Google's fair-use defence.

The US Congress has codified the fair-use defence, which permits the use of copyrighted work without the copyright owner's consent. Much American jurisprudence stands for the proposition that this defence must be interpreted in a flexible manner and be similarly applied, calling for a case-by-case analysis. On the

facts of this case, the court discussed the significantly transformative nature of Google's search engine, especially given its public benefit, which, in the court's view, was more important than Google's incidental superseding and minor commercial use of the thumbnails in question. This factor ranked as one of the most important among many used to determine Google's use of the thumbnails as being fair use, in light of the purpose of copyright law in the U.S.

The court then continued on an analysis of secondary liability for copyright infringement. Using the *Grokster* case, it said that Perfect 10 must prove Google's activities intentionally induced or encouraged direct infringement. The two ways in which this may occur are (i) actively encouraging or inducing infringement through certain specific acts or activities or (ii) distributing a product whose use is to infringe copyright. On the second element, the court quickly concluded that Google cannot be held liable for contributory infringement based solely on the design of the search engine. That would be absurd. Rather, the court concentrated on the first category (intentionally encouraging infringement through specific acts).

The question before the court was therefore whether Google knowingly took steps that are substantially certain to

result in such direct infringement. In the parallel *Napster* case, the court held that if a computer system operator has knowledge of infringing material and fails to delete the content from the system, it contributes to direct infringement. Under this reasoning, intent can be imputed. In the case at hand, the court relied on these above two cases and said that Google indisputably assists both websites in distributing infringing copies to a worldwide market and users in accessing infringing material. Since the lower court failed to analyze this point in detail and look at reasonable and feasible means for Google to curb access to infringing images, this claim has been remanded to it for further consideration.

Contact [Barry Sookman](mailto:bsookman@mccarthy.ca) in Toronto at bsookman@mccarthy.ca

Europe: Significant Win for Music Industry versus ISPs

In what is being hailed as a rather large victory for the music industry in Europe, a court in Belgium has held a Belgian ISP responsible for blocking illegal file sharing on its network. The court of first instance has ordered the ISP to install technology within the next six months to prevent users from sharing pirated music and video files. A failure to do so will result in stiff daily penalties. This will set a precedent in the industry because musicians and their associations have been fighting to hold ISPs accountable for their part in illegal Internet

file sharing. Though the movement in the U.S. has been largely unsuccessful, this European decision may have major consequences around the world.

McCarthy Tétrault Notes:

The decision was mostly based on the court's interpretation of the EU Copyright Directive. ISPs have long argued that, as service providers, they ought not to be responsible for the dealings of others. However, the ruling is a step forward for the International Federation of the Phonographic Industry (IFPI), which says that the ruling confirms that ISPs have a legal responsibility and the technical means to tackle the widespread efforts of online piracy. The technical means to which the IFPI refers are based on a study recommended by a Belgian court in 2004, where an appointed expert studied the technical options available to ISPs and concluded seven specific ways for technology to help curb piracy, including one that creates a digital fingerprint for each copyrighted work.

Of note, of course, is the possibility of appeal in this case, although it is unclear whether the ISP will appeal the decision.

Contact [Barry Sookman](mailto:bsookman@mccarthy.ca) in Toronto at bsookman@mccarthy.ca

TRADE-MARKS

U.S.: Utah Legislation for 'Electronic Registration Marks' Delayed

In February 2007, the Utah legislature approved legislation establishing a new type of 'electronic registration mark.' The legislation amends the state's *Trademark Protection Act* and is intended to target the practice of advertisers bidding on or buying keywords that reflect competitors' trade-marks, in order to trigger the display of their advertisements when the competitor's trade-mark is searched using a search engine.

The legislation passed without a dissenting vote, and despite a statement from the Utah State General Counsel that it offered a high probability of being challenged in court and found unconstitutional. It had initially been set to take effect on April 30, 2007. It was subsequently reported in the press that implementation would occur on June 30, 2007. However, following a late-April meeting between legislators and objecting search engine representatives (including Google, AOL, Yahoo, Microsoft and others), the Utah governor has reportedly delayed implementation of the legislation for at least several months. Changes to the legislation are currently being considered.

McCarthy Tétrault Notes:

Potential for challenge

News reports alleged that Google had been considering filing a lawsuit in opposition to the legislation. Google's position was that US law does not forbid advertisers from attempting to gain their competitors' customers, and that it does prohibit use of a rival's trade-mark in content of advertising text. However, it allows advertisers to bid on the right to use a competitor's brand as a search keyword to trigger display of advertising. Google had also reportedly offered to target advertising to a city level, based on a consumer's Internet Protocol address. However, it did not address concerns that such technology is imperfect and would not address the issue that other third-party advertising platforms may not operate with Google's level of technology or sophistication.

Meanwhile, at the time the legislation was passed, a legislative review note had also been released by the Utah State Legislature (Office of Legislative Research and General Counsel). The note stated that because the amended Act is aimed at the use of user-entered search terms to trigger advertisements, a state's regulation of keywords on an Internet search engine may potentially impact interstate commerce. The legislation may therefore have a high probability of being found to be unconstitutional.

What the legislation says

In its current form, the legislation's general description states that it establishes a "new type of mark, called an electronic registration mark, that may not be used to trigger advertising for a competitor and creates a database for use in administering marks."

It aims to make illegal the use of a competitor's keyword or phrase to trigger an advertisement online. Practically, the legislation may result in the requirement that search engines check a database of electronic registration marks to avoid displaying offending ads, in addition to checking every advertisement request to see if the advertiser or seller was based in Utah, in case of electronic registration conflicts. Some key points to consider include the following:

- The goal is to prohibit the use of an electronic registration mark to trigger advertising for a business, goods or services of the same class as those represented by the electronic registration mark.
- 'Electronic registration mark' is defined as "a word, term or name that represents a business, goods or a service."
- An application for an electronic registration mark can be filed using similar information as a trade-mark application (including goods/services,

date of first use anywhere and in commerce), and two specimens and a fee (to be determined, up to a maximum of US\$250 annually for one class, with additional classes at a maximum of US\$25 each annually). The registration division *may* request that the applicant provide a statement confirming whether an application for the mark or portions thereof has been filed with the United States Patent and Trademark Office (USPTO) and any related information, including reasons for refusal or lack of registration.

- The legislation does not appear to provide for substantive prosecution objections, or challenge or oppose applications.
- The legislation does not appear to provide for cancellation procedures other than expiry due to failure to renew. (Note: A statement of use must be submitted in order to renew an electronic registration mark.)
- An electronic registration mark typically has a five-year term (renewable for additional five-year terms).
- No sunrise period is provided for owners of trade-mark registrations with the USPTO to file corresponding applications for electronic registration marks.

- The legislation allows for civil action for acts involving the use of the electronic registration mark to “cause the delivery or display of an advertisement” (with similar classes of goods or services or in a way likely to cause confusion), if display of the advertisement is in the state or the advertiser or seller is located in the state. No specified criteria exists for establishing likelihood of confusion.
- The legislation provides that no damages are recoverable unless there is intent to cause “confusion or mistake” or to “deceive.”
- The legislation provides for the creation and maintenance of a searchable database of marks by the Division of Corporations and Commercial Code (within the Department of Commerce).

Comment

Theoretically, the legislation addresses a serious concern of trade-mark owners for whom courts have not definitively settled the issue of use of their marks by competitors as keyword advertising. Court actions in recent years have yielded inconsistent rulings, some of which are overturned on appeal.

Practically, the legislation raises many questions for both advertisers and trade-mark owners in Utah and elsewhere. Would the display of a website viewable in Utah that

advertises goods or services be considered the display of an advertisement in Utah? How well will electronic registration marks and the system for applications and registrations in the USPTO coexist? How could a trade-mark owner (particularly a common law mark owner) challenge or oppose an electronic registration mark? Will electronic registration mark applications be prosecuted substantively, or will they be granted as long as formal filing requirements are met? Would the legislation prevent reasonable comparative advertising, and/or availability to consumers of comparative information? Would the legislation survive a legal challenge? Will other jurisdictions follow suit?

In the end, it may be prudent at least for those whose businesses have a connection with Utah to preserve their rights by applying for electronic registration marks reflecting their trade-marks once the legislation comes into force, and to monitor the evolution of this legislation.

Contact [Jeanette Lee](#) in Toronto at jwlee@mccarthy.ca

PATENTS

U.S.: Supreme Court Hands Down KSR Ruling

On April 30, 2007, the US Supreme Court issued its unanimous decision in *KSR International Co. v. Teleflex Inc.* In it, the Supreme Court reversed the decision of the Court of Appeals for the Federal Circuit and restored the decision of the District Court, which had rejected a claim of patent infringement. The Supreme Court held that the allegedly infringed patent was invalid on the grounds that it was obvious in light of prior art.

McCarthy Tétrault Notes:

Section 103 of the US *Patent Act* prohibits the issuance of a patent where “the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art.”

The framework for applying section 103 was set out by the Supreme Court in *Graham v. John Deere Co. of Kansas City*. To paraphrase the test from that case, the differences between the prior art and claims at issue, along with the level of ordinary skill in the pertinent art, must first be resolved. Against this background, the obviousness of the subject matter is determined. To illuminate the origin of the subject matter sought to be patented,

secondary considerations may include commercial success, long-felt (but unsolved) needs and failure of others.

Additionally, the Court of Appeals has adopted a test called the ‘teaching, suggestion or motivation’ (TSM) test in an attempt to impose more consistency with respect to the application of the test for obviousness. In the TSM test, a patent claim would only be found obvious where the prior art, the problem’s nature or the knowledge of a person having ordinary skill in the art reveals some motivation to combine the prior art teachings.

In this case, the claim at issue described a mechanism for combining an electronic sensor with an adjustable automobile pedal. At issue was whether affixing this electronic sensor to a fixed point was obvious, given that the device was known in the art to have adjustable automobile pedals with fixed pivot points, and to use electronic sensors with automobile pedals to control acceleration of an automobile. The Supreme Court agreed with KSR that mounting the sensor on a fixed pivot point was a design step well within the grasp of a person skilled in the relevant art. The District Court found that the patent was obvious, but the Court of Appeals overturned this decision, applying the TSM test and concluding that the patent was not obvious.

In the *KSR* decision, the Supreme Court overturned the Court of Appeals, soundly criticizing the Court of Appeals’ “narrow

conception of the obviousness inquiry reflected in its application of the TSM test.” As explained in a memo from the Deputy Commissioner for Patent Operations to the Technology Center Directors of the United States Patent and Trademark Office, the Supreme Court did not completely reject the TSM test, but did reject a strict application of the TSM test that would require, for a finding of obviousness, that the prior art show some teaching, suggestion or motivation that would lead one skilled in the art to combine the prior art references.

The Supreme Court explained that “the obviousness analysis cannot be confined by a formalistic conception of the words teaching, suggestion, and motivation, or by overemphasis on the importance of published articles and the explicit content of issued patents.” Pursuant to KSR, an analysis of prior art need not involve seeking out “precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ.” Moreover, if patents are granted with respect to advances that would occur in the ordinary course without real innovation, this may impede progress, and may also, in the case of patents that combine previously known elements, deprive those prior inventions of their value or utility, according to the Supreme Court.

This is an important decision because the test for obviousness has become easier to satisfy. As such, it will likely result in more rejections based on obviousness issuing from the examiners at the USPTO, as well as, potentially, more issued patents being found to be invalid on grounds of obviousness.

The decision may also result in increased difficulty for patent holders in enforcing patent rights in the U.S., because alleged infringers may be able to challenge more effectively the validity of the patents that the patent holders seek to assert.

Contact [Ian Bies](#) in Toronto at ibies@mccarthy.ca

Privacy

CASES/LEGAL DEVELOPMENTS

Canada: **Committee Recommends Amendments to Canada's Federal Privacy Legislation**

On May 2, 2007, the Standing Committee on Access to Information, Privacy and Ethics presented to the House of Commons its report arising from the statutory review of the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA).

The Committee's recommendations reflect extensive consultations with various stakeholders and mostly represent a fine-tuning of PIPEDA rather than wholesale amendments. As noted by the Committee, much of the fine-tuning is premised on the need for greater harmonization between PIPEDA and the laws of the provinces of Québec, Alberta and British Columbia, all of which have substantially similar private-sector data-protection laws. Various stakeholders' submissions to the Committee argued that British Columbia's and Alberta's "'second generation' privacy laws provide a more practical and updated reflection of privacy protection today."

The following are some highlights from the recommendations:

1. Amend PIPEDA to include a breach notification provision requiring organizations to report certain defined breaches of their personal information holdings to the Federal Privacy Commissioner.
2. Include a provision permitting organizations to collect, use and disclose personal information without consent for the purposes of a business transaction.
3. Include a definition of 'work product' that is explicitly recognized as not constituting personal information.
4. Clarify the form and adequacy of consent required by PIPEDA, distinguishing between express, implied and deemed/opt-out consent.
5. Incorporate amendments to address the collection, use and disclosure of personal information in the employment context.
6. No amendments should be made to PIPEDA with respect to transborder flows of personal information.
7. The Privacy Commissioner should not be granted order-making powers at this time.
8. No amendment should be made with respect to the Privacy Commissioner's discretionary power to publicly name organizations in the public interest.

McCarthy Tétrault Notes:

Many of the changes recommended by the Committee will be welcomed by organizations that are subject to PIPEDA's privacy protection requirements.

First, many of the proposed changes would address compliance obligations that have proven unwieldy to organizations that are subject to PIPEDA. One example is the failure of PIPEDA to permit the collection, use and disclosure of personal information about employees without consent, as is required to manage the employment relationship. The absence of such an exemption to the consent requirements of PIPEDA has proven a challenge for federally regulated employers.

Second, many of the amendments would have the practical effect of harmonizing PIPEDA with the current provincial privacy legislation (such as British Columbia's or Alberta's *Personal Information Protection Act* or Québec's *An Act Respecting the Protection of Personal Information in the Private Sector*). For example, introduction of an exemption for 'work product information' and further definition of PIPEDA's exemption for business contact information would enhance the ability of organizations that operate in multiple provinces to implement consistent privacy practices and processes throughout Canada.

Many organizations will also welcome the Committee's recommendation that no

amendments be made to PIPEDA with respect to transborder flows of personal information. Consistent with the recommendations of the Privacy Commissioner of Canada, the Committee noted that "[PIPEDA] already contains sufficient accountability and allows for the necessary flexibility for businesses to ensure that personal information is privacy protected when it crosses our borders," and encouraged the Commissioner to continue providing guidance to organizations regarding the implementation of appropriate safeguards.

Another hot topic the Committee considered was whether PIPEDA should be amended to expressly require that organizations report breaches of privacy – that is, in circumstances in which personal information under the control of the organization has been subject to unauthorized access or use. Despite the potential drain on resources that such a mechanism could put on the Commissioner's office and despite the lack of power to make binding orders, the Committee recommended a requirement that organizations report certain defined breaches to the Commissioner. The Commissioner would in turn determine whether affected individuals and others should be notified and, if so, in what manner. This approach differs from that taken in other jurisdictions, including many US states, which require direct notification of the affected individuals in the event of certain breaches.

Although it will be some time before the Committee's recommendations translate into amendments to PIPEDA, organizations should at the very least revisit their internal privacy processes to ensure that an internal escalation mechanism has been implemented. This mechanism should include requiring service providers to notify of breaches relating to personal information that has been provided to the service providers by the organization and ensuring that IT staff, risk management professionals, human resources personnel and other relevant individuals are prepared to respond to breaches.

Contact [Cappone D'Angelo](mailto:cdangelo@mccarthy.ca) in Vancouver at cdangelo@mccarthy.ca

Contact [Catherine Samuel](mailto:csamuel@mccarthy.ca) in Calgary at csamuel@mccarthy.ca

Contact [Wendy Gross](mailto:wgross@mccarthy.ca) in Toronto at wgross@mccarthy.ca

Contact [Barbara McIsaac](mailto:bmcisaac@mccarthy.ca) in Ottawa at bmcisaac@mccarthy.ca

Contact [Charles Morgan](mailto:cmorgan@mccarthy.ca) in Montréal at cmorgan@mccarthy.ca

Canada: Disclosure of Personal Information without Consent Pursuant to Lawful Authority

Sometimes businesses receive requests for personal information from the police or other law enforcement bodies and must then consider whether they may disclose the requested information in light of the *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA states that the knowledge and consent of an individual are generally required for the collection, use or disclosure of personal information about him or her. However, the Act sets out some exceptions to allow disclosure of personal information without the individual's knowledge or consent. The Ontario Court of Justice recently provided some clarification about one such exception found in s. 7(3)(c.1) of PIPEDA.

McCarthy Tétrault Notes:

This provision states that an organization may disclose personal information without consent to a government institution that has made a request for the information, identified its "lawful authority" to obtain the information and indicated that the disclosure is requested for the purpose of enforcing, investigating or gathering intelligence for the enforcement of a law of Canada, a province or a foreign jurisdiction. Section 7(3)(c.1) appears to allow disclosure in situations other than just in response to a subpoena or warrant or when "required by law," as separate provisions (s. 7(3)(c) and s. 7(3)(i)) provide for disclosure without consent in such circumstances. In Re

S.C., the Ontario Court of Justice offered some guidance about the scope of the “without consent” exception in s. 7(3)(c.1).

This decision appears to indicate that in order to rely on the exception in s. 7(3)(c.1), the “lawful authority” to obtain the information must first be established by the government institution, and that PIPEDA itself does not establish the authority for it to obtain the information. Unless that lawful authority is established, a private sector entity (in this case, Bell Canada) may risk falling afoul of PIPEDA by disclosing the information unless some other “without consent” exception applies.

Re S.C. considered a request for a search warrant and whether there was sufficient authority for the Toronto Police Service to have obtained subscriber information and addresses from an information service provider. Prior to seeking a warrant to search an individual’s home, the police had requested subscriber information for the user of a certain Internet protocol address from Bell Canada. The letter stated that the “request was done under the authority of PIPEDA.” Bell Canada supplied information to the investigators.

However, the Justice of the Peace found that the information supplied in the request for a search warrant was information for which a citizen would have a reasonable expectation of privacy. Accordingly, there was a presumption based on the *Charter of Rights and Freedoms* that prior judicial authorization was required to obtain such

information via a search warrant or production order.

Accordingly, Bell Canada did not have a basis upon which to disclose the information, and the information obtained was set aside in the overall consideration of the search warrant application because the police were not lawfully in possession of it. The request for the search warrant was ultimately rejected because the balance of the information obtained did not establish a reasonable nexus between the matters being investigated and the individual and residence identified as targets for the warrant.

In light of this clarification of the law, it appears that a company subject to PIPEDA should take the following steps when faced with a request for personal information from a government institution conducting an investigation or enforcing a law:

- if the institution does not have a subpoena, warrant or court order, advise that the company may have obligations under PIPEDA in respect of the information requested;
- request that the institution specify its lawful authority to obtain personal information; and
- check the authority cited in order to satisfy itself that the institution has lawful authority to obtain the information.

Contact [Howard R. Fohr](#) in Ottawa at hfohr@mccarthy.ca

Canada: **Computers and the Emergence of Privacy Breaches**

Several recent high-profile privacy breaches have begun to focus the attention of corporate Canada on the important legal issues that result from the disclosure of personal information of customers or employees in an unauthorized manner through loss or theft. What is the liability of a company when data is inadvertently disclosed? Should the company inform the affected data subjects, and if so, when? What steps should be taken to minimize the damage to the company's reputation? And how can future privacy breach incidents be better managed?

McCarthy Tétrault Notes:

These are all good questions. But before turning to them, consider some of the broader trends that are behind our current vulnerability to privacy breaches. It's no coincidence that the volume and severity of these incidents are increasing. To understand why, reflect for a moment on the history of computing and networking over the past 40 years, particularly from the perspective of the challenges posed to computer security and data privacy by the principal phases of computing technology over this period.

The low-risk mainframe

During the first wave of computerization in the 1960s and 1970s, each organization's IT system consisted of one (or more)

centralized mainframe computer (aka the 'big iron'), which was operated in the bowels of the company by a handful of people. The mainframe stood alone and wasn't connected to other computers at the company, let alone to computers at other companies.

Computer security in such an environment was fairly straightforward. So long as the small team running the computer was honest, very little harm could come to the computer or the data residing on it. This computing environment did not raise many privacy-breach challenges, at least from a security perspective.

IT diffusion

Ever since the appearance of the mainframe computer, engineers have been hard at work trying to replace it with smaller, more versatile computing machines. By the early 1980s, so-called mid-range computers had found favour in company IT strategies. These computers also had strings of dumb terminals (called 'dumb' because they did not do processing themselves but could at least access the mid-range computer that did the heavy lifting) attached to them. Lo and behold, these terminals found their way onto the desks of secretaries at the company. And so began the inexorable democratization of computing.

Mid-range computers and their concomitant dumb terminals showed companies the huge promise of distributed computing.

Many new applications began to be used by the non-IT staff of the company (or other organizations, such as government departments) using these powerful new hardware machines. Of course, from a privacy and security perspective, this new computing configuration meant that more people in the organization had access to sensitive customer and employee data. One bad-apple employee now had the potential to access a myriad of company data.

From office to home

By the mid-1980s, computer democratization was picking up pace with the advent of the personal computer. Before long, there was a computer on every desk in an organization. And these weren't merely dumb terminals; smaller and more powerful microchips allowed them to process data themselves, though they were also connected to hub computers called servers.

Moreover, the PC revolution wasn't confined to the office. Soon, these powerful but fairly compact devices insinuated themselves into the home. Floppy disks containing large gobs of data began travelling between the PC at the office and the one at home. Not surprisingly, the first serious incidents of data loss were reported as floppies were inadvertently mislaid, or worse, stolen.

The Internet changes all things

In the mid-1990s, of course, everything changed with the coming of the Internet. Personal computers, servers and even

mainframes could now all be networked, both within proprietary/closed systems or, increasingly, through non-proprietary open ones such as the Internet. For the first time, computers became data-communication devices as well as data-processing machines.

Computer crime has been with us since the beginning of the computer revolution. Canada's *Criminal Code*, for example, was amended some 20 years ago to deal expressly with computer-related offences. Nevertheless, the Internet gave rise to a whole new type of computer criminal, the so-called hacker, and a whole new ease by which to penetrate remote computer systems. In a word, the Internet made information more vulnerable.

Wireless, everywhere

In the last 10 years, computing devices have become smaller, more powerful and cheaper. The PC begat the laptop, which in turn (along with the cell phone) gave birth to the personal digital assistant, such as the BlackBerry.

The microprocessor, however, is no longer used only in standalone computers. Rather, together with digitally-based sensors, microprocessors are being implanted into huge numbers of machines and objects as diverse as bridges and – dare I say – even people. And what makes all this computer power even more compelling is that the sensors and chips can send their data to host computers through the ether without

having to be tethered by wires. Consider a few of the state-of-the-art applications.

The digital mousetrap

In the UK, a building maintenance firm has rigged mousetraps with digital sensors and microchips. Thus, when a rodent is caught, the firm learns about it in real time. Also, as the different traps 'report in,' the firm can detect quickly if one of the buildings is perhaps experiencing an outbreak of the little critters (and can go investigate why). Even short of this important news, the information received from the traps simply teaches the firm where to put additional mousetraps, and when to check on them.

While the data security and privacy implications of the digital mousetrap may not be readily apparent (though the track record of each building in this regard may indeed be very sensitive business information, with commercial implications for the landlord), consider the following new wireless computing applications that bristle with privacy law implications.

On the digital highway

Again in the UK, a car insurance company has unveiled an insurance product that provides much more granular pricing based on very detailed, real-time car usage patterns, which are tracked and processed by computers. So, if you drive down a highway on a Sunday (which is quite safe, surprisingly), you pay a lot less insurance

for that trip than you would for a drive downtown during a weekday rush hour.

This is a good example of what more and more miniature microprocessors can do: They can tell us, in real time, what is going on around them. Other current new applications include a school in Japan that is putting wireless homing devices on young children so that the school never loses track of them. Similarly, a North American uniform maker is putting chips into firefighters' suits so that their position can be determined at all times while they are fighting a large blaze, such as in a large, multi-storey warehouse.

Under my skin

A range of digitally driven, wireless-connected medical devices is also hitting the market. Small chips with long-lasting power devices are being implanted just under the skin of various patients to facilitate monitoring of various vital statistics or collect more nuanced data. Essentially, these are tiny radio frequency identification tags that let doctors monitor their patients from afar.

These digital implant technologies will not long be restricted to the health community. Indeed, one bar in Spain embeds such chips in patrons' arms to assist with identity verification and payment. Previously the stuff of James Bond movies, these digital, wireless implant devices will grow into a huge business in a matter of years.

Security and privacy implications

These technology trends and the business models generated by them have profound implications for Canadian privacy law. In a nutshell, all the examples touched on above involve the collection of huge amounts of data, largely of the sensitive, personal variety. And this data is then transmitted hither and yon, over a variety of networks and by means of various technologies. While all of this activity brings significant benefits, there is of course one inevitable downside.

With so much data being collected, stored, processed and transmitted, it's merely a question of time before some of your data leaks out, notwithstanding the implementation of 'best practices' procedures for security and privacy. And so the question can reasonably be asked: How does the current legal regime deal with privacy breaches? It is this topic that will be discussed in the next TLQ.

Contact [George S. Takach](mailto:gtakach@mccarthy.ca) in Toronto at gtakach@mccarthy.ca

Canada: New Electricity Technologies and Their Privacy Implications

In California, an exciting program aimed at managing increasing electricity consumption levels is raising serious concerns about privacy. Demand Response, an initiative recently adopted by legislators in the U.S., promises to eliminate the need for new power plants, saving billions of dollars. Yet the cutting-edge technology required to make the program truly effective has caught the attention of legal analysts and privacy advocates.

McCarthy Tétrault Notes:

Demand displaced

Although their implementation takes various forms, demand-response programs generally involve consumers shifting their use of electricity to different times of the day, namely to off-peak usage periods. For example, residential users could engage in their energy-consuming morning rituals at 5 a.m., or some time after 9 a.m. Similarly, they could refrain from using their air conditioning units for part of the time between 6 p.m. and 9 p.m.

The advantages of demand response are best understood by adopting a 'weakest link in the chain' analogy. In order to be reliable, the electricity infrastructure must be capable of satisfying demand at all times of the day, and in particular, at the times of day during which consumption is highest. In this context, its reliability is

only as good as its capacity to meet demand during peak periods, even if that capacity isn't needed for most of the day. As electricity consumption levels have increased over the years, so has peak-period usage. Eventually, building new power plants would have to be built to satisfy demand.

If enough users shift their consumption to off-peak periods, electricity consumption levels at peak periods might not increase as much as they otherwise would, and might actually remain constant or decrease. As a result, governments and utilities would save money by not having to build new power plants. Most importantly, under a demand-response program, these savings could be realized even if overall consumption remained the same. The Demand Response and Advanced Metering Coalition argues that Americans can save over \$10 billion thanks to demand-response programs.

Government-sponsored attempts to persuade people to change their habits have a mixed record, but utilities and legislators have found several creative ways to convince consumers to shift their electricity usage. In California, residential and commercial users can volunteer to participate in various demand-response programs; under one scheme, residential users can have their utility company automatically turn off their thermostats for 15 minutes each hour. In exchange, the users receive rebates on their electricity bills.

Advanced metering technology

The true innovation of Demand Response arises from utilities charging consumers different rates for electricity consumption based on the time of day, with prices rising during peak periods. This creates an incentive for consumers to shift their usage. At its most dynamic, utilities could vary electricity rates on a real-time basis rather than establish rates in advance, much in the same manner that the price of an airline ticket changes throughout the day. The US Congress formally endorsed this approach when it amended the *Energy Policy Act* in 2005. Section 1252 of the Act requires utilities to offer, upon request, "a time-based rate schedule under which the rate charged by the electric utility varies during different time periods."

For this to happen, however, dramatic technological changes need to take place. Indeed, they are well under way, in the form of advanced metering technology. The vast majority of consumers in both Canada and the U.S. use conventional electricity meters that record usage on a monthly basis and do not allow utilities to adopt more dynamic pricing models. The new generation of meters are capable of recording electricity consumption continually throughout the day, at intervals as small as 15 minutes, transmitting data wirelessly to the utility's central office. In this way, consumers who use electricity during off-peak periods can record their use and benefit from lower rates.

What about the Fourth Amendment?

Legal scholars and privacy advocates in the U.S. are concerned about the implications of this new technology for the right to privacy protected under the Fourth Amendment of the US Constitution and under state constitutions. In a forthcoming article for the *Stanford Technology Law Review*, Deirdre K. Mulligan and Jack Lerner note that the information transmitted by the new electricity meters is qualitatively very different from the monthly readings taken on the conventional devices. Specifically, if data on electricity consumption were transmitted every hour and subsequently stored for long periods (as many utilities are required to do), considerable information could be gained about the daily habits of consumers. Electricity consumption patterns could be used to determine when consumers were home, their level of activity at various times of day and whether they made use of specialized medical equipment. Activities taking place purely within the privacy of the home and previously inaccessible to the outside world could be exposed to a wider audience.

The Fourth Amendment entrenches “[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,” and requires government officials to obtain authorization before carrying out a search of the premises. The Fourth Amendment was long understood in the narrow sense of physical entry into the

home. From this view, police officers could use a camera to capture a suspect’s movements and not violate the Fourth Amendment if they never actually entered the home.

The US Supreme Court departed from this approach 40 years ago in *Katz v. United States*. In that case, the FBI placed an electronic listening device on a public telephone booth and recorded a suspect’s conversations, without having obtained a warrant. The suspect was convicted and successfully appealed under the Fourth Amendment. The court noted that “the Fourth Amendment protects people, not places,” from unreasonable search and seizure, and the fact that the electronic device did not physically penetrate the telephone booth was irrelevant. The court also dismissed the government’s argument that Katz could not invoke the Fourth Amendment because he used a public telephone, holding that what a person “seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.” In the wake of *Katz*, the Fourth Amendment guarantee has been interpreted broadly and remained relevant with advances in technology.

Yet, advanced metering technology remains a cause for concern in the U.S., due both to a nuance in the court’s reasoning in *Katz* and to subsequent decisions. Although it held that information could remain private even if it were in a public area, the court added that “[w]hat a person knowingly

exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection." Accordingly, in *Smith v. Maryland*, it held that when people voluntarily give information to a third party, they "assume the risk of subsequent disclosure."

This reasoning raises the real possibility that the government could access detailed data on an individual's activities within the privacy of his or her home that, in the absence of advanced metering technology, would have required a warrant. The consumption habits of electricity users could, following transmittal, become simply part of a utility's business records.

Coming to Ontario by 2010

Demand Response is far from a purely American phenomenon. Ontario has already implemented a demand-response program and will have installed 800,000 'smart electricity meters' by the end of this year, with the objective of having transitioned all consumers by 2010. The smart-meter technology consists of two components: an Advanced Metering Infrastructure (AMI) and a Meter Data Management and Meter Data Repository (MDM/R). The AMI collects hourly electricity consumption data and transmits it to the utility's central computer. The data are then transferred to the MDM/R, which compiles billing records. Consumers would be able to access their consumption data on an ongoing basis, making it easier for them to adjust their habits.

Ontario's Ministry of Energy has held consultations on the implementation of the smart-meter technology and acknowledged that privacy is a concern. Canadian tax law requires that data be stored for at least seven years, since they are used for billing purposes. Feedback gathered on this topic during the consultations underscored the need to set out clear guidelines on the information that will be stored and the level of access granted. Yet, privacy concerns do not appear to have become a great concern; a spokesperson for Ontario's Office of the Information and Privacy Commissioner interviewed for this article said that her office had yet to receive a single complaint about the implications of smart-meter technology.

Watch this space

It is difficult to argue with the underlying principles of demand-response programs; even the most passionate privacy advocates acknowledge the benefits of smart meters. Although the programs seem so far to have raised greater privacy concerns south of the border than in Canada, new technologies are renowned for provoking legal debates unimagined at the time of implementation.

Contact [George S. Takach](mailto:gtakach@mccarthy.ca) in Toronto at gtakach@mccarthy.ca

Contact Verki Tunteng in Toronto at vtunteng@mccarthy.ca

Communications

CASES/LEGAL DEVELOPMENTS

Canada: **Model Act to Implement Telecom Sector Reform Released**

Lawyers in our Communications Group, led by senior partner Hank Intven, released a *Model Telecommunications Act* containing detailed legislative provisions that could be used to implement key recommendations of the March 2006 report of the *Telecommunications Policy Review Panel* (TPR Report). The Model Act was prepared by Mr. Intven, who was a member of the panel, and Mary Dawson, former Associate Deputy Minister of Justice.

McCarthy Tétrault Notes:

The TPR Report called for major reforms of the policy and regulatory framework for the Canadian telecommunications industry. Since release of the report, the federal government has moved quickly to implement many of its recommendations, particularly those aimed at deregulation of the telecommunications industry, which the Panel described as urgent. However, the report ultimately called for a comprehensive set of reforms, including new legislation, creation of new competition and consumer watchdog agencies, and clear guidelines for when regulators should, and should not, intervene in telecom markets.

The purpose and intent in creating this Act is to give the government, Parliament and other industry stakeholders, including consumers, some ideas and practical suggestions on how one might start the difficult job of drafting new telecom legislation to implement the TPR Report.

Contact [Hank Intven](#) in Toronto at hintven@mccarthy.ca

Canada: **Voice over IP Services – Regulatory Perspectives from the Developed and Developing Worlds – Part II**

This article continues our four-part series focusing on the regulatory issues surrounding voice over Internet protocol (VOIP) services. It analyzes some fairly recent CRTC VOIP decisions and follows up on VOIP regulatory concerns in the developed world.

McCarthy Tétrault Notes:

The CRTC has rendered two decisions dealing with the issues raised by Telecom Public Notice CRTC 2004-2.

The Emergency Services Decision

On April 4, 2005, the CRTC released Telecom Decision CRTC 2005-21. In that decision, the CRTC made its final determinations regarding the emergency

service issues raised in Telecom Public Notice CRTC 2002-2.

In the Emergency Services Decision, the CRTC confirms its position that the public interest requires imposing emergency service obligations on local VOIP service providers. By contrast, a VOIP service offering providing only long-distance calling capability would not be subject to these obligations. Only VOIP services that provide a substitute or functional equivalent to local public switched telephone network services are to be subject to the identified emergency service obligations.

The Emergency Services Decision examines the special complications associated with the nomadic and non-geographic capabilities of VOIP services, and resolves these complications by examining three different ways in which VOIP services can be deployed:

- from a fixed address with a telephone number that is native to one of the exchanges within the customer's PSAP (public-safety answering point; i.e., within its service area);
- from a fixed address with a telephone number that is not native to one of the exchanges within the customer's PSAP service area (i.e., where the assigned telephone number is identified with an exchange that is outside the geographic area of the subscriber's registered service address); and

- on a nomadic basis, where the customer makes calls from an address that is different from the registered address for service.

For services associated with a fixed address and a telephone number that is native to the public safety answering point service area, the CRTC expects VOIP service providers to be able to supply emergency services practically equivalent to those for conventional local service offerings, including participating in the exchange of all required subscriber information and related data. For non-geographic and nomadic services, the CRTC requires VOIP service providers to implement appropriate interim solutions that provide a level of emergency service comparable to the basic emergency services provided by conventional service providers. This includes using the intervention of call centre agents to confirm the location of the caller and to ensure that the call is transferred to the appropriate PSAP or emergency service best able to respond to the emergency and subscriber location.

The CRTC has also asked the industry steering committee responsible for resolving competitive market issues – namely, the CRTC Interconnection Steering Committee (CISC) – to submit a report identifying the technical and operational issues that impair emergency services where local VOIP service is offered on a non-geographic basis, and a similar report within one year with respect to service offered on a nomadic basis. In

addition to identifying the practical problems of implementing emergency services in these circumstances, the reports will identify alternative solutions, make recommendations for preferred solutions and propose time frames for implementation.

Finally, the Emergency Services Decision emphasizes the importance of informing potential subscribers of all emergency service limitations prior to any VOIP service commitment, and requires express acknowledgement by subscribers of these service limitations as part of the process of contracting for VOIP services.

The regulatory framework decision

On May 12, 2005, the CRTC issued telecom decision CRTC 2005-28, resolving the remaining issues raised by Telecom Public Notice CRTC 2004-2.

This decision deals with the issues raised by Public Notice CRTC 2004-2 that were not dealt with in the Emergency Services Decision. Most importantly, this decision sets out the CRTC's final determinations regarding the regulatory framework that should apply to VOIP services, including the extent to which those services should be forborne from conventional regulation.

VOIP service categories

The Regulatory Framework Decision begins with a discussion of various categories of VOIP services.

One category of service that the CRTC singles out for specific treatment is 'peer-to-peer' or 'P2P' services, which it defines as "IP-enabled voice communications services that do not connect to the public-switched telephone network and that do not use conventionally assigned telephone numbers." These peer-to-peer services include computer-to-computer voice communications with traffic routed via the Internet and without using a conventional telephone number or related switching to establish the voice connection. The CRTC considers these peer-to-peer VOIP services to be within the category of retail Internet services, a service category that it has previously determined should be forborne from regulation.

The FCC has also determined that these peer-to-peer communication services are not subject to traditional telecommunications regulation by either the FCC or state regulatory commissions, on the basis that they constitute regulation exempt 'information services' and do not constitute 'telecommunication services.'

Forbearance from regulation

Under its governing legislation, Canada's *Telecommunications Act*, the CRTC has the power to forbear from regulation where it determines that markets are sufficiently competitive or that forbearance would otherwise be in accordance with the policies set out in the Act. In its Regulatory Framework Decision, the CRTC confirms

that VOIP services, other than peer-to-peer services, are not within the category of 'retail end user Internet services' previously forborne from tariff and other regulation. The CRTC bases that determination on characteristics of VOIP services that distinguish them from retail Internet services. Ultimately, the CRTC finds that the primary function of VOIP services is not accessing the Internet, but rather accessing the public-switched telephone network in order to make and receive telephone calls.

Having determined that local VOIP services are not within existing forbearance determinations, the CRTC also considers specific requests by the incumbent telephone companies to grant new forbearance orders regarding local VOIP services. The CRTC examines these requests for forbearance in accordance with a methodology based primarily on consideration of the relevant market for local VOIP services, and whether firms in that market have sufficient market power to maintain prices above those that would prevail in a competitive market.

In performing this analysis, the CRTC finds that local VOIP services satisfy the same general requirements as circuit-switched local exchange services and are close substitutes for those circuit-switched services. Accordingly, local VOIP services are part of the same relevant market as conventional circuit-switched local services. The CRTC includes 'access-

independent' VOIP service configurations in this finding that local VOIP services are part of the same relevant market as conventional local services.

The CRTC also notes that the incumbent local exchange carriers in Canada remain dominant providers of local service, accounting for 98 per cent of local residential revenues and 92 per cent of local business revenues in 2003. Given the definition of the relevant market, and the continuing market share of incumbent carriers, the CRTC concludes that it would not be appropriate to forbear from tariff and other regulation of local VOIP services offered by incumbent carriers at this time.

The CRTC also considers whether cable television companies provide sufficient competition to incumbent carriers in local VOIP or other voice services markets to support forbearance. It observes that although the cable companies are emerging as stronger competitors, they remain subject to obstacles compared with the incumbent carriers, including the need to (i) upgrade conventional cable networks to permit the delivery of VOIP or other voice services (ii) accumulate experience in offering local voice services over time.

The CRTC also expresses concern about the competitive advantage enjoyed by incumbent carriers in their ability to migrate existing customers from conventional telephone services to VOIP services, particularly given their

continuing dominance in conventional local service markets. Another concern is that granting forbearance from tariff regulation prematurely could permit incumbent carriers to engage in targeted below-cost pricing of local VOIP services, and related bundling strategies, permitting them to continue their market dominance prior to the entry of other competitors.

Ultimately, the CRTC denies the request for forbearance from the regulation of local VOIP services and determines that local VOIP services should be regulated as local exchange services, including application of the CRTC's previously determined regulatory framework governing local service competition (as modified by other parts of the decision).

Application of local service regulatory framework

Having dealt with the request for regulatory forbearance, the CRTC examines specific issues in the application of its regulatory framework for local service competition to local VOIP services in the balance of the decision.

The CRTC's determinations include confirmation that the existing framework for the allocation of telephone numbers, and rights and obligations pertaining to local number portability, apply to local VOIP service providers on the same basis as conventional local service providers. Similarly, the requirements of directory

information and subscriber listing information remain generally the same. The only difference is that directory listings for VOIP service subscribers are to appear in the local directory where calls to or from the assigned number are local calls regardless of the location of the subscriber's service address. Local VOIP service providers are also subject to the general obligation to ensure equal access to competitive long-distance service providers. They must not enter into contractual arrangements or otherwise obstruct access by their subscribers to competing long-distance service providers.

Regarding Message Relay Service and other disability services, the CRTC concludes that local VOIP service providers should offer comparable service capabilities to the extent that is technically feasible. It also asks the CISC to prepare a report addressing technical problems and recommended solutions for the implementation of these disability functions.

Similarly, the CRTC determines that privacy safeguards such as blocking of calling line identification and disabling of call return should be implemented by local VOIP service providers to the extent that is technically feasible. Again, it requests the CISC to assess the technical issues associated with implementing these privacy safeguards using VOIP technologies and service configurations.

Regarding tariff-filing requirements, the CRTC confirms that incumbent carriers

must file tariffs for local VOIP services within their traditional geographic operating territories. Outside these territories, where the incumbent carriers do not exercise market power, the carriers will have the benefit of tariff regulation forbearance. Similarly, non-dominant carriers that do not have market power in a geographic market will not be required to file tariffs for local VOIP services so long as they generally comply with the requirements of being a competitive local exchange carrier.

As indicated previously in this article, in Telecom Public Notice CRTC 2002-2, the CRTC made a preliminary determination that VOIP services should be subject to the same obligation to support the cost of telecommunication service in high-cost areas (the 'contribution' mechanism used in Canada to achieve universal service objectives). In the Regulatory Framework Decision, the CRTC confirms this preliminary determination and provides further guidance on the extent to which revenues from VOIP services should be contribution eligible. Generally, the CRTC confirms that the revenues for services that permit access to and from the public-switched telephone network are to be contribution-eligible, and that revenues associated with peer-to-peer voice communications (i.e., computer-to-computer and other communications that do not use conventional numbering to make a connection) are not contribution eligible. The CRTC also confirms that local VOIP

service providers will be entitled to the benefit of contribution-fund subsidies to extend service into high-cost service areas where they meet the basic service characteristics defined for conventional local service.

Finally, the regulatory framework decision includes determinations requiring cable companies and telecommunications carriers to remove contractual restrictions that prohibit the offering of voice communication services from their terms of service for ISP resellers. The intention of this further determination is to ensure that ISPs making use of cable television systems or telephone company facilities or services are able to offer voice communications as part of their competing service offerings.

Concluding comments

As indicated earlier in this article, the issues raised by the CRTC in its VOIP Public Notice are similar to issues that have been raised by the FCC and OFCOM in their own VOIP public notices and proceedings. The issues include the extent to which VOIP services and service providers should be subject to the regulatory framework established for local and long-distance voice services generally, particularly given the underlying technologies and service characteristics of VOIP services.

The CRTC's recent decisions are among the first efforts by a regulator to deal with these issues in a market with a history of extensive voice service competition.

It remains to be seen whether the CRTC's determinations on VOIP issues will be repeated by the FCC, OFCOM or other regulators examining the issues in similar service environments.

For its part, the CRTC has taken the position that VOIP services should be subject to the same regulatory framework as conventional telephone services, to the extent that VOIP services provide unrestricted access to and from the public switched telephone network, make use of the same numbering conventions and otherwise provide consumers with services that are practically equivalent to conventional telephone services.

The CRTC has, however, recognized that VOIP service platforms are not at present able to reproduce all of the emergency services, disability access and other service characteristics of conventional circuit-switched telephone services. The CRTC has adopted the pragmatic stance of requiring VOIP services to meet these public requirements as soon as technologically feasible, with specific interim measures applicable until that time, particularly including disclosure to consumers of the service limitations.

The regulatory challenges faced by countries that do not have a history of extensive service competition, and where the state of development of telecommunications network facilities and services is more limited, are very different.

These will be explored in the third instalment of this four-part article.

Contact [Stephen Rawson](#) in Toronto at srawson@mccarthy.ca

Biotechnology/ Life Sciences

CASES/LEGAL DEVELOPMENTS

Canada: **Renegotiating University Biotechnology Licenses**

Many biotechnology companies are spin-offs from universities and other academic institutions, such as research centres or hospitals. While the founders of these biotechs very often continue to hold positions with their academic institutions, the intent of creating the spin-off is to run it as a private business. The result is an interesting clash of cultures between the academic and business worlds. Educational and research institutions value academic and scientific publication of research and the open dissemination of technology for societal advancement. They also operate on a not-for-profit basis. By contrast, private business stresses maintaining the market value of the technology through obtaining exclusive rights to the technology and conducting controlled exploitation in order to generate maximum profits.

McCarthy Tétrault Notes:

Of course, the reality is seldom as clear-cut as the foregoing suggests. Academic institutions have become used to earning money from biotechnology spin-offs. Thus, technology development offices often behave much like private sector licensors

in matters such as granting exclusives in return for higher royalties, valuing technology based on industry norms and guarding the secrecy of their business and financial terms to preserve their negotiation leverage in dealings with private-sector licensees. However, real differences exist nonetheless between institutional and private-sector biotechnology licensing, which derived from their different normative frameworks. At the spin-off stage, many of these differences will be tilted in favour of the academic institution. The closer the technology is to pure science (as opposed to a commercialized drug), the more embedded it will still be in the academic and research culture. Moreover, at the spin-off stage, the institution often holds greater power in the negotiations for a number of reasons:

1. The institution owns the technology and decides when and if it will be commercialized. Since the institution's 'business' is research and education, drug commercialization is a sideline and the institution can often afford to wait for the right terms before licensing.
2. Academic institutions are highly risk averse and will not assume risks that private businesses consider normal.

3. To a certain extent, institutions that spin off technology are acting outside of their element. They may not be entirely comfortable in a business environment and therefore may be inflexible on negotiation points that would contain 'gives' in pure business deals.
4. Spin-off companies are often created by the scientists who invented the technology and who continue to work at the institution. They do not always seek independent business and legal advice, nor fully appreciate the need for that advice.

However, if the science bears promise and development proceeds, the nearing prospect of commercializing the technology will bring greater weight to business concerns. In particular, incoming investors or partners may require amendments to the original license as a condition of investing or may make payment of future development and commercial milestones to the spin-off conditional upon amendments being made to the original institution license. Accordingly, biotechs often need to renegotiate their original licenses with the institution.

Frequently renegotiated terms

Although there is no limit to the possible terms that a biotech may wish to renegotiate with its licensor institution in the context of a particular financing

or partnering transaction, some of the more common ones are considered below.

Ownership of improvements made by the licensee – In the initial stages of a biotech spin-off, it may be staffed and run by persons holding appointments at the institution. There may be good reasons in these circumstances for improvements to the licensed technology made by the licensee to be owned by the institution (and licensed back to the spin-off). However, once the spin-off reaches the stage of wishing to enter into development collaborations with drug partners, the partners will expect the collaboration improvements to be owned jointly by the collaboration, or solely by the collaborator if made by the collaborator. The ownership rules of the original license therefore need to be rewritten at this stage. A possible compromise might involve governing of the ownership of collaboration according to the rules of inventorship (i.e., jointly by the collaborators if made jointly or solely by a party if made solely, but in any case, not assigned back to the institution), but with collaboration improvements remaining royalty-bearing vis-à-vis the institution if commercialized.

Royalties – Original royalty rates, often set early in the scientific stages of development, may need to be revised to account for a deeper understanding of the intellectual property environment and partnering prospects for the technology.

Development and commercialization milestones – Development and commercialization milestones in early stage licenses are very often ‘best guesses.’ After a few years of development of the technology, more sophisticated and equitable milestones can be devised.

Patent prosecution – Institutional licenses will very often provide that the institution itself will conduct intellectual property prosecution and maintenance. When the spin-off reaches a higher level of business maturity, these responsibilities are very often taken over by the spin-off.

Confidentiality provisions – Confidentiality and publication provisions of institutional licenses may not be sufficiently broad for disclosures required by securities laws and stock exchange policies, particularly if the spin-off becomes a public company, or for disclosures to drug regulators in connection with development of the technology.

Governance restrictions – Institutional licenses may include governance restrictions on the spin-offs, which reflect of the institution’s desire to be involved in their spin-offs’ activities and the perceived need for the institution’s technology development office to tutor their early-stage spin-offs in business matters. Dealers and partners will typically require such restrictions to be removed so that they can impose their own restrictions.

Termination rights – Institutional licenses sometimes have multiple hooks into the licensed technology that, if triggered, will give rise to termination rights in favour of the institution. This reflects the high failure rate of biotechnology companies and the resulting interest of the institutions to recover the technology in order to re-license it to other prospects if the original licensee fails or doesn’t perform. Once the biotech has reached a more mature stage of corporate development and financing, strong arguments can be made that these hooks by the institution into the intellectual property should be removed in order to place the spin-off on a stronger and more independent footing.

Sublicensee protection – An institutional license will very often provide that sublicenses will terminate if the head license with the spin-off terminates. This term may impede the ability of a successful spin-off to partner the technology. It therefore may be renegotiated to provide protections to collaborators of the spin-off, such as the right to obtain a license directly from the institution if the spin-off’s head license fails.

Assignment of intellectual property – It may be possible to negotiate assignments of intellectual property from the institution in lieu of the original license. Intellectual property assignments would generally require the spin-off to be on a strong business footing at the time of the renegotiation.

Conclusion

Many biotech spin-offs from academic or research institutions find themselves either wanting to renegotiate their licenses or being required to do so by investors or partners. For their part, the institutions are tied to the success of their spin-offs and will have a strong interest in placing the license on terms that work for the spin-off. Legal and business advisors experienced in working in the nexus of the academic and business worlds can play a large part in these renegotiations by knowing where the 'gives' are for the institutions and which terms of institutional licenses (as idiosyncratic as they may appear to private business) are non-negotiable for the institutions. The result can very often be 'win-win' renegotiations for both the institution and the spin-off.

Contact [Paul Armitage](mailto:parmitage@mccarthy.ca) in Vancouver at parmitage@mccarthy.ca

Clean Technology

CASES/LEGAL DEVELOPMENTS

Canada: Clean Technology Coming of Age

This article begins an interesting four-part series on clean technology and its impact in today's society. For some, clean technology is a passion. For others, it's a commitment to their children and grandchildren. But for most of the players in the clean tech space, it's about 'doing good business,' which includes making money.

Clean tech is broadly defined as knowledge-based products or services that improve operational performance, productivity or efficiency while reducing costs, inputs, energy consumption, waste or pollution. For example, clean tech includes alternative energies (such as wind and solar power), information technology, fuel cells, hybrid vehicles, biomass, biofuels, lighting and energy-efficient household appliances.

McCarthy Tétrault Notes:

It's difficult to underestimate the impact and potential of clean tech. Venture capitalists are increasingly investing in this area, which is significant because these investments are leading indicators of future economic growth. Many large global corporations have or are developing sustainability plans. The World Business Council for Sustainable Development is a

CEO-led council of 200 of the world's largest corporations ranging from insurance to petroleum companies with a collective market capitalization of over \$5 trillion. Traditional industry sector companies such as Alcan, Transalta, BC Hydro and Suncor, as well as Oracle and IBM from the information technology sectors, participate in the World Business Council. The purpose of the Council is to develop strategies and provide thought leadership in dealing with sustainability and climate change from a business perspective. In addition to venture capital (VC) and direct business investment, governments are developing policies and funding incentives at the federal, provincial/state and municipal levels to promote clean tech adoption and foster development of those technologies.

North American VC investment in clean tech has more than doubled in the past two years to \$2.9 billion, which makes it the third-largest category after biotech and computing. GE alone intends to double its current clean tech VC investment to \$50 million by 2008 – and these are just the investments by its VC group. GE's bigger plan is to double its overall investments in clean tech and renewable energy to \$4 billion by 2010. During the first quarter this year, \$237 million was invested in alternative energy deals in the US alone. For those who are counting, this represents the lion's share of this quarter's VC investment in the clean tech category.

Investment categories go through a number of phases as they evolve. Current data indicates that clean tech is emerging as a defined investment category at twice the pace of biotech's rise in the 1980s and early 1990s. With the combination of rising energy costs, overall natural resource scarcity, growing demand for environmentally superior products and greatly improved clean tech alternatives, clean tech may capture up to 10 per cent of overall venture capital flows by 2009. It may also capture an increasingly large portion of both M&A and IPO activity. A clean tech market index, called the Cleantech Index (CTIUS) and traded on the American Stock Exchange, tracks this sector and represents approximately \$300 billion of market capitalization.

Clean tech investment is ramping up through VC funding, public markets and government incentives. This funding is being consumed primarily by new business opportunities and traditional businesses retooling, and all business interests are optimizing for predicted consumer and social change. New business opportunities are arising, mainly in technology-related areas such as renewable energy, alternative fuels, water treatment, power storage and conditioning, and demand-side management tools.

Sustainability is a key driver in how traditional businesses evolve their products, services and approach to doing business, such as innovations relating to energy and water

usage improvement in oil sands extraction. Several other traditional businesses, such as financial institutions, are also taking on clean tech and sustainability principles. Citigroup has committed to spend \$50 billion over the next 10 years to address global climate change, and this year, the Bank of America launched a 10-year \$20-billion green plan. Even icons of the information technology industries, including Google, are exploring alternatives to reduce their global footprint by providing for alternative energy solutions for energy-intensive aspects of their businesses, such as server farms.

Sustainability is also becoming an aspect of corporate governance for directors and senior executives. Initially, the focus covers the areas of risk management, corporate social responsibility and corporate reputation. Rising public awareness and sustainability concerns are effecting changes in business practice in certain traditional industry sectors. Engaging local communities and obtaining the legitimacy of a 'social license' from that community is now becoming standard practice. The Canadian mining industry has played a leadership role in setting global standards in this area.

In this article, we focused on VC and capital flows into the clean tech space. In the next *Technology Law Quarterly*, we will discuss the impact of clean tech and sustainability in traditional businesses and on corporate governance.

Contact [Cheryl Slusarchuk](#) in Vancouver at cslusarchuk@mccarthy.ca

VANCOUVER

P.O. Box 10424, Pacific Centre
Suite 1300, 777 Dunsmuir Street
Vancouver BC V7Y 1K2
Tel: 604-643-7100 Fax: 604-643-7900

CALGARY

Suite 3300, 421 - 7th Avenue SW
Calgary AB T2P 4K9
Tel: 403-260-3500 Fax: 403-260-3501

TORONTO

Box 48, Suite 4700
Toronto Dominion Bank Tower
Toronto ON M5K 1E6
Tel: 416-362-1812 Fax: 416-868-0673

OTTAWA

The Chambers
Suite 1400, 40 Elgin Street
Ottawa ON K1P 5K6
Tel: 613-238-2000 Fax: 613-563-9386

MONTREAL

Suite 2500
1000 De La Gauchetière Street West
Montréal, QC H3B 0A2
Tel: 514-397-4100 Fax: 514-875-6246

QUEBEC

Le Complexe St-Amable
1150, rue de Claire-Fontaine, 7e étage
Québec QC G1R 5G4
Tel: 418-521-3000 Fax: 418-521-3099

UNITED KINGDOM & EUROPE

5 Old Bailey, 2nd Floor
London, England EC4M 7BA
Tel: +44 (0)20 7489 5700 Fax: +44 (0)20 7489 5777

The right people. The right results.®

McCarthy
Tétrault

VANCOUVER • CALGARY • TORONTO • OTTAWA • MONTRÉAL • QUÉBEC • LONDON, UK

MCCARTHY.CA

Every effort has been made to ensure the accuracy of this publication, but the comments are necessarily of a general nature, are for information purposes only and do not constitute legal advice in any matter whatsoever. Clients are urged to seek specific advice on matters of concern and not rely solely on the text of this publication.