

IT.CAN NEWSLETTER

Canadian IT Law Association

www.it-can.ca

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

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

Digital Cameras and Privacy Rights

The British Columbia Court of Appeal had occasion to comment on the privacy significance of digital cameras with their decision in *R. v. Caron*. The accused had been arrested for dangerous driving after an officer clocked him going 165 kph in a 100 kph zone. After handcuffing the accused and placing him in the rear of the police vehicle, the officer opened the accused's glove compartment and found a digital camera. The officer then looked through the images on the camera, testifying that he thought the accused might have taken a picture of his speedometer showing a high rate of speed. In fact the officer saw pictures of the accused holding firearms, which led him to search the car, discovering \$60,000 and a pistol. He was charged both with dangerous driving and with a firearms offence.

The Crown conceded that the police officer's search of the digital camera had violated the accused's section 8 right, and the real issue in the case was whether the evidence should be excluded. In looking at that question, the court considered the impact of the breach on the accused's *Charter*-protected interests, finding it to be very high. They held:

60 We live in an age in which digital cameras, either standing alone or as a component of other electronic devices such as smartphones, have become ubiquitous. Those cameras allow individuals to record personal, and sometimes, intimate aspects of their lives and those of their family and friends, in a manner that would not have been contemplated in the days when the common way for most people

to take photographs was with a camera using film that had to be given to a third-party to develop and print. Today, for some people, a digital camera may serve as an electronic journal or diary. In other words, these cameras often contain "biographical core" personal information that an individual is entitled to keep private: *R. v. Plant*, [1993] 3 S.C.R. 281 at 293; *R. v. Tessling*, 2004 SCC 67, [2004] 3 S.C.R. 432 at paras. 25, 26.

61 Given the nature of the information stored in digital cameras, I consider the unreasonable examination that occurred in this case to be far more than a minimal interference with Mr. Caron's right to privacy. That Constable Roberts scrolled through the camera's memory quickly does not lessen the gravity of that intrusion.

Due Diligence and the Do Not Call List

The Canadian Radio-television and Telecommunications Commission (CRTC) has rendered a decision with regard to administrative monetary penalties for violations of the Unsolicited Telecommunications Rules, popularly known as the "Do Not Call" list (DNCL). The penalty was awarded against [Direct to Home Groceries](#) with regard to five voice telemarketing telecommunications to consumers who were registered with the Do Not Call list and five voice telemarketing telecommunications without being a registered subscriber or having paid all applicable fees to the National DNCL operator. The total penalties normally payable in connection with these violations would be \$10,000.

Direct to Home Groceries submitted that they had not knowingly contacted the consumers, and that the communications had occurred as a result of a computer glitch. They also sought a reduction in the penalty, if they were found to be in violation, on the basis that a \$10,000 penalty would put them out of business.

The Commission concluded that the issue of the computer glitch would only be relevant to the question of whether Direct to Home Groceries had established a defence of due diligence. They had earlier established criteria giving guidance on how to establish such a defence, which included that the caller have written policies and procedures on how to avoid calling consumers on the DNCL, training programs for employees, and that the caller not use lists which had not been updated for more than 31 days. The Commission concluded that the claim of a computer malfunction was not sufficient to establish a claim of due diligence.

This was particularly so given that Direct to Home Groceries had not submitted any additional evidence of other reasonable steps or any business practices that could demonstrate due diligence, and that they had continued to make telemarketing telecommunications to consumers whose numbers were registered on the National DNCL after its subscription had expired.

With regard to the amount of the administrative monetary penalty and the possibility that it would put Direct to Home Groceries out of business, it was held:

15. The Commission notes that the financial health of a corporation is not a factor in determining whether to impose or reduce a penalty contained in a notice of violation.

Accordingly they ordered that the full \$10,000 penalty be paid.

Searches for Electronic Data

In *R. v. Ballendine*, the accused was charged with possession of child pornography. The investigation into him had begun with an investigation by Europol into a child pornography distributor in Italy, through which email addresses of customers around the world who had ordered DVDs had been discovered, including that of the accused. From that information the police had identified the accused and had obtained a search warrant for his home. That warrant authorized the police to search for and seize the DVDs which he had ordered, but it also authorized them to search and seize any computers and computer-related equipment. The police did not in fact find any of the DVDs the accused had ordered from Italy. However, a forensic examination

of his computer hard drive disclosed a large number of other child-pornography videos, as well as a short clip from one of the DVDs he had ordered. In addition the examination of another hard drive showed visits to child-pornography websites.

The accused objected to the search warrant on a number of bases, including that the telewarrant procedures had been improperly used, that some of the evidence presented consisted of conclusory statements by the investigating officer, and others, none of which succeeded. Two objections are of particular relevance for our purposes.

First, the accused argued that the terms of the warrant were too broad in allowing for the seizure of computers. The accused argued that the information to obtain at best established grounds to show that he was in possession of DVDs containing child pornography, and therefore that the warrant ought only to have authorized searching for DVDs. The British Columbia Court of Appeal was unpersuaded by this claim:

61 It is common knowledge that things such as correspondence, financial records, photographs and videos are stored on computers. As Dufour J. stated in *Wonitowy* at para. 46, “[c]omputers have been around long enough that expert evidence explaining their most basic function as a storage device is not required”. This being so, it was open to the justice of the peace to conclude there were reasonable grounds to believe that someone who appeared to be a collector of child-pornography videos would likely have copied all or some of those videos onto his computer.

In addition, the Court of Appeal held that the search of the computers could be relevant in other ways, such as to connect the accused to the purchase of the DVDs through emails, or through documents that connected the accused to the location. They noted that evidence of occupancy or residency is relevant to establishing a possession claim, and that documents connecting the accused to the location would be relevant. In that event, the police were not limited to searching for hard copies of such documents:

63 ...they equally had grounds to search for electronic versions of those things. An

electronically-stored version of a letter or photograph that connects a person to premises is as cogent a piece of evidence as a hard-copy of the same thing.

A further claim made by the accused was that the warrant obtained by the police entitled them at most to seize the computers, but not to conduct a search of their contents: a further warrant would have been required for that, he argued. The Court of Appeal however, concluded that this was not a case where a computer simply happened to be swept up in a search conducted of premises under a warrant. Rather, the justice of the peace was made aware of the fact that there were reasonable grounds to believe that a computer had been used in the commission of the offence and that it would be found in the location for which the warrant was issued. He had also been made aware that an on-site forensic examination of any computer found would be impracticable. In addition, the warrant specifically named computers as one of the things for which the police were entitled to search and seize. In those circumstances, the court held, the warrants should be taken not only to authorize taking the computers away from the scene, but also to allow the police to conduct a forensic examination of them to locate any electronically stored data.

British Injunction Gags Twitter and Facebook

World media are [reporting](#) that Justice Baker of the United Kingdom Court of Protection (a superior court division which handles the financial affairs and personal welfare of those deemed to lack mental capacity to make decisions for themselves) has issued a publication ban which specifically targets social media. The case is that of M, a 43-year old woman who has been hospitalized with encephalitis since 2003, existing in a vegetative state. Her mother has applied to the court for an order halting the measures being taken to preserve M's life. The publication ban, apparently issued to protect the family's privacy, restricts people from approaching the woman or her family, but also explicitly forbids the publication of identifying information in "any newspaper, magazine, public computer network, internet site, social network or media including Twitter or Facebook, sound or

television broadcast or cable or satellite programme service." One [commentator](#) referred to the order as being "among the first [British] injunctions specifically referring to Twitter and Facebook." While not seemingly controversial itself, the publication ban has re-emphasized criticisms of the private nature of some British court proceedings, as well as a controversy over wide-ranging injunctions taken out by media figures to prevent Twittering on their lives and activities.

Belgian Court Rules Google News Infringes Belgian Copyright

In the recent case of *Google Inc v Copiepresse et al.*, the 9th Chamber of Belgium's Court of Appeals (Brussels) has ruled that Google's "Google News" service infringed copyrights held by Belgian authors and publishers by offering content to Belgian customers at google.be and google.com (The only available report of the case, at the above hyperlink, is in French, but an English summary and expert commentary can be found [here](#)). The claimants were Belgian copyright holders who had published content on Belgian websites. Google News indexed and cached articles published by the claimants and made available titles and excerpts via google.be and google.com, both of which were transmitted via servers in California. Users could access the articles via the google sites, even though some might otherwise have been taken down or subject to fees for access on their original Belgian sites. The claimants argued that the indexing, caching and reproduction all violated various aspects of Belgian copyright law, including interfering with moral rights and rights of reproduction.

The Appeals Court first ruled that Belgium had jurisdiction over the matter and that Belgian copyright law applied, even though many of Google's acts had taken place in California, because Belgium was the state with the closest connection to the overall transaction and because the articles had been transmitted to Belgium. The authors, in particular, had suffered violations of both their rights of paternity (because the author's name did not appear with the excerpts when generated) and their rights of integrity (because the excerpting of the articles meant that they had been republished in a modified

form, without the authors' permission). The Court rejected Google's argument that the defence of fair dealing applied, ruling that the exceptions in Article 5.5 of the EU Copyright Directive could not be met. It further rejected Google's argument that there was an implied license for its activities since the copyright holders had not opted out of the Google News service, as well as the argument that it was the users of Google News that were actually responsible for the reproduction and communication of the content.

Domain Name Decisions

"ultimatefightingchampionships.ca"

In *Zuffa, LLC v. David Bruce*, sole CIRA panelist David Lametti heard a dispute regarding the domain name ultimatefightingchampionships.ca. The Complainant ("Zuffa") is a Nevada-based corporation which produces and promotes mixed martial arts fighting events in Canada and internationally. It registered the mark ULTIMATE FIGHTING CHAMPIONSHIP in Canada in 2005, and used the mark in association with its services as early as 1993. It has also registered design marks incorporating the marks THE ULTIMATE FIGHTING CHAMPIONSHIP and ULTIMATE FIGHTING CHAMPIONSHIP UFC. The Registrant ("Bruce") is an individual who resides in Kelowna, BC. He registered the domain name on 25 February 2008, but has left it displaying an "under construction" graphic since. He did not respond to the complaint in a procedurally appropriate manner. Prior to the complaint the parties had various communications in which Zuffa offered to purchase the domain name for \$2500 and tickets to an event. Bruce responded that his expenses for maintenance had been \$2600, that he had registered the name in order to "make a profit," and that he had registered seven other domain names using the ULTIMATE FIGHTING CHAMPIONSHIP mark. He hoped that Zuffa would make a "bulk offer" for all of the domain names.

As Zuffa had met the Canadian presence requirement and had established rights in the mark that pre-dated registration of the domain name (under 3.2 of the CIRA Policy), Panelist Lametti turned first to whether the domain name was "confusingly similar" to Zuffa's mark, noting that the "distinctive elements of the domain name and the trademark are identical." It

was therefore "confusingly similar," since it "is well-established that neither pluralization nor a change in spacing is a significant difference mitigating against a finding of confusing similarity" (para. 23). Turning to whether the domain name had been registered "in bad faith" under 3.7 of the Policy, the Panelist held that bad faith had been made out under both 3.7(a) and (b) of the Policy. The former finding was that Bruce had taken out the registration primarily for the purpose of selling it to Zuffa, as evidenced by Bruce's admissions in his e-mails that he hoped to profit from such a sale and was aware of the notoriety of the mark, as well as by the fact that no content was ever added to the site. The latter finding was that Bruce had intended to prevent Zuffa from registering the domain name itself, as evidenced by the fact that he had engaged in a pattern of registering domain names containing trademarks belonging both to Zuffa and to other organizations.

The final determination by the Panelist was that there was evidence that Bruce had "no legitimate interest" in the domain name per 3.6 of the Policy. He remarked: "This inquiry tries to find some more or less objective or ascertainable link between the Registrant and the domain name in question, aside from mere registration, and which is legitimate" (para. 29). A finding of "no legitimate interest" was ultimately grounded on Bruce's admission that he was aware of Zuffa and its interests, the lack of content on the site, and the lack of evidence that Bruce could fall under any of the criteria of legitimate interest in 3.6 of the Policy. Since Bruce had not responded to the complaint, he could not meet the burden of leading evidence to the contrary which had shifted to him. Zuffa's complaint was successful and the domain name ordered transferred to Zuffa.

Electronic Research in Costs Order

In *Fairchild v. Vancouver Coastal Health Authority*, Registrar K.S. Sainty of the B.C. Supreme Court was assessing costs in a medical malpractice action that had settled. The plaintiff had claimed disbursements for, inter alia, electronic legal research in the amount of \$360 (Westlaw) and \$444.95 (Quicklaw). The Registrar cited her own decision in the 2001 case of *Prevette v. Cusano*, wherein disbursements for

electronic research were denied because of the availability of a free database of B.C. court decisions. She then remarked:

I am even more convinced today that the cost of computerised research is properly an item of overhead than I was in 2001 when I decided *Prevette v. Cusano*. In this current electronic age there are even more resources available (at no cost) for conducting legal research online than ever before (for example, there is now the CanLii system and our own courts website — which includes the vast majority of the court’s written reasons issues since 1999, at least). Therefore absent convincing evidence that pay-per-use type of computerised legal research was a necessary adjunct of the prosecution of this

case, I will not allow the claim for these amounts (para. 78).

In the result, the Westlaw disbursements were allowed because counsel had used a specialized personal injury database relating to quantum, which the Registrar felt was “reasonable and necessary” (para. 80). However, the Quicklaw expenses were disallowed, the Registrar remarking: “it is true that in some cases, QuickLaw is a necessary and proper disbursement. But that is not a given. There must be some evidence justifying its use. Here, I was not told why QuickLaw searches were necessary or proper or why searches could not have been conducted using free online services, as opposed to a pay-per-use service such as QuickLaw” (para. 81).

This newsletter is intended to keep members of IT.Can informed about Canadian legal developments as well as about international developments that may have an impact on Canada. It will also be a vehicle for the Executive and Board of Directors of the Association to keep you informed of Association news such as upcoming conferences.

If you have comments or suggestions about this newsletter, please contact Professors Robert Currie, Chidi Oguamanam and Stephen Coughlan at it.law@dal.ca.

Disclaimer: The IT.Can Newsletter is intended to provide readers with notice of certain new developments and issues of legal significance. It is not intended to be a complete statement of the law, nor is it intended to provide legal advice. No person should act or rely upon the information in the IT.Can Newsletter without seeking specific legal advice.

Copyright 2011 by Robert Currie, Chidi Oguamanam and Stephen Coughlan. Members of IT.Can may circulate this newsletter within their organizations. All other copying, reposting or republishing of this newsletter, in whole or in part, electronically or in print, is prohibited without express written permission.

Le présent bulletin se veut un outil d’information à l’intention des membres d’IT.Can qui souhaitent être renseignés sur les développements du droit canadien et du droit international qui pourraient avoir une incidence sur le Canada. Le comité exécutif et le conseil d’administration de l’Association s’en serviront également pour vous tenir au courant des nouvelles concernant l’Association, telles que les conférences à venir.

Pour tous commentaires ou toutes suggestions concernant le présent bulletin, veuillez communiquer avec les professeurs Robert Currie, Chidi Oguamanam et Stephen Coughlan à l’adresse suivante : it.law@dal.ca

Avertissement : Le Bulletin IT.Can vise à informer les lecteurs au sujet de récents développements et de certaines questions à portée juridique. Il ne se veut pas un exposé complet de la loi et n’est pas destiné à donner des conseils juridiques. Nul ne devrait donner suite ou se fier aux renseignements figurant dans le Bulletin IT.Can sans avoir consulté au préalable un conseiller juridique.

© Robert Currie, Chidi Oguamanam et Stephen Coughlan, 2011. Les membres d’IT.Can ont l’autorisation de distribuer ce bulletin au sein de leur organisation. Il est autrement interdit de le copier ou de l’afficher ou de le publier de nouveau, en tout ou en partie, en format électronique ou papier, sans en avoir obtenu par écrit l’autorisation expresse.