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

June 16, 2011

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.

Continuity of Digital Photographs

The Nova Scotia Court of Appeal has considered the issue of continuity of digital photographs and videos with its decision in *R. v. Murphy*. The accused faced trial on 43 charges of theft, break, enter and theft, possession of stolen property and weapons offences, following a series of police raids at five residential sites in the course of which over 2,000 items of stolen property were recovered. At the end of the trial the accused was acquitted of 32 of those charges, all of which related to break, enter and theft, or possession of stolen property. The trial judge had refused to admit various evidence, which included surveillance video from the scene of some of the thefts and digital photographs taken by police of many of the recovered items, and therefore found that the Crown had not proven the accused's guilt beyond a reasonable doubt. The Crown appealed, and the Court of Appeal granted the appeal, holding that the trial judge had erred in refusing to admit the evidence, and ordering a new trial.

One piece of evidence was a surveillance video tape from Kent Building Supplies, from which an electronic fireplace had been stolen. The Crown called the loss prevention supervisor from the store in order to introduce the video, which was on a CD. The accused objected, asking for proof of continuity and proof that the CD which was present in court was the same CD which the loss prevention supervisor had given to the police. In the absence of the loss prevention officer's initials on the CD, for example, the accused argued that it could not be admitted. The Crown acknowledged that it was not possible to tell from the exterior of the CD what it contained, but proposed to play the beginning of it in order to allow the witness to identify it. The trial judge, however, refused to allow this: he judge found that since there were no identifying markers on the disk to allow the witness to objectively identify it without reviewing its content, the "evidential threshold" for admissibility had not been met and the video was inadmissible.

The Court of Appeal found this to be an error, for several reasons. First, the observed that "[i]t is difficult to understand how the trial judge expected the witness to authenticate the contents of the video without accessing it" (para 30). Second, they noted that videotape of a theft can be self-authenticating: a trier of fact is entitled to view the video and form an opinion on whether it shows the accused committing the offence. Finally the trial judge confused the issue of whether continuity of the exhibit had been demonstrated with the question of whether the exhibit was admissible.

The Court of Appeal also overturned rulings by the trial judge with regard to digital photographs which were taken of many of the recovered items. The Crown initially tried to introduce these photographs by way of affidavit, but the affidavits were ruled inadmissible. The Crown then called a police officer who had taken the photographs on one of the CDs. She explained the process she had undertaken in taking the photographs, comparing them for accuracy, storing them, and then reorganizing them for the purpose of burning the CD. She also testified that she had reviewed the photographs to ensure that they were accurate depictions as she burned the CD.

The accused, however, had objected that the CD could not be accessed unless the Crown first proved the number of photographs on it and the dates they were. The trial judge agreed, and ruled that the CD could not be accessed without there first being proof of those matters in order to establish continuity. He also held, as with the video, that proof of continuity

of the photographs had to be established beyond a reasonable doubt for them to be admitted

Again the Court of Appeal overturned this decision, for two reasons. First, they held that the trial judge had erred in taking the "beyond a reasonable doubt" standard to apply to the admissibility of an individual piece of evidence: the photographs did not themselves have to be proven beyond a reasonable doubt in order to be admissible and contribute to proof beyond a reasonable doubt of the elements of the offence. Further, the trial judge had again confused continuity and admissibility. The photographs could be found admissible even if they were not introduced through the person who took them, provided that they accurately and truly represented the facts, were fairly presented and without any intent to mislead and were verified on oath by a person capable of doing so. If there were an issue over continuity that might affect the weight given to the evidence, but it did not render them inadmissible.

The Court of Appeal concluded that these errors could well have affected the trial judge's ultimate decision, and therefore ordered a new trial.

Google and Privacy

The Office of the Privacy Commissioner of Canada has found Google to be in violation of PIPEDA with its report on Google Inc. WiFi Data Collection.

The issue arose through actions of the Google Street View cameras, and in fact affected many more countries than just Canada. The Street View Camera vehicles were equipped with the ability to collect publicly broadcast WiFi data. The intention was to collect service set identifier (SSID) and MAC addresses, but in addition, in the case of unsecured networks, it had also been capturing payload data. These payload data included names, telephone numbers and addresses, complete email messages, IP addresses, instant messages and chat sessions, usernames and passwords, and more. Because the vehicles were in motion as they captured data and regularly changed channels, much of this information was so fragmentary that it could not have identified individuals and therefore was not "personal information" under PIPEDA. Some of it, however, was.

Google collected this data for roughly three years before it discovered that it was doing so. At that point it grounded its Street View cars, stopped the collection of WiFi network data, segregated and stored all the data collected, and notified government and law-enforcement officials of the incident, including the Privacy Commissioner.

Three complaints under PIPEDA were investigated. That Google:

1. collected personal information not limited to that which was necessary for purposes identified by the organization
2. collected the personal information of individuals without first identifying and disclosing the purposes for which that personal information was to be collected; and
3. collected the personal information of individuals without their knowledge and consent.

Fairly straightforwardly in the circumstances, the Privacy Commissioner found all three complaints to be justified. Google, in that it was accidentally collecting the information and did not contest that it was doing so, was collecting information which was unnecessary, without disclosing the purpose, and without consent. The greater question was what to do going forward, given that the data was no longer being collected.

The Privacy Commissioner raised concerns that the privacy implications of the software with which the Street View vehicles were equipped had not been sufficiently obvious to the Google engineers who developed it. In addition, the code was not reviewed for its privacy impacts at the time it was reviewed to become operational. Finally Google had collected the data for three years before the issue had come to light.

The Privacy Commissioner concluded that:

> We believe that the issue is more than one of simple oversight however. The lack of concern for privacy issues emanating from the engineer's code, and the cursory privacy reviews conducted by managers during the code's acceptance and integration suggest, in our view, a far greater problem at Google.

> Notwithstanding the promise of its founding Privacy Principles, the incident in question suggests that Google employees may be suffering from a lack of privacy training and awareness. The company may also be lacking appropriate management structures to ensure privacy accountability.

The Commissioner did commend Google for the way in which it responded to the privacy breach when it was discovered, and noted that it already intended to destroy the data, but that the process needed to be undertaken in accordance with the laws of several countries. Google had also commenced a review of its privacy procedures and policies, and had commenced new online training modules for all Google employees, some specifically addressing data security and privacy, as well as training programs specifically tailored to address privacy in the context of Google's Engineering, Product Management, People Operations, Sales and Legal functions. Google had also committed to undertaking various other measures to ensure that privacy was better protected.

The Privacy Commissioner concluded that if all of these measures were implemented, it would satisfy all the concerns which had arisen. The Commissioner gave Google a period of twelve months to complete undertaking those measures, and intended to meet with the corporation over that period of time to monitor the implementation. In addition the Privacy Commissioner requested that Google undergo and share the results of an independent, third-party audit of its privacy programs within one year.

Defamation via E-mail

In *Wright v. Van Gaalen*, Justice Schultes of the British Columbia Supreme Court dealt with commercial litigation that involved, *inter alia*, a claim for defamation allegedly accomplished by e-mail. Both parties were designers of fire suppression systems and had entered into a partnership in order to take advantage of some lucrative work opportunities; the litigation arose from the acrimonious dissolution of the partnership. At a point at which the winding-up of the partnership had become particularly difficult, the defendant Van Gaalen sent an e-mail to Williams (the principal of Ablaze, a firm which was a longstanding client of the plaintiff Wright), but which was addressed in the body of the e-mail to Brown (the principal of TG, a firm which was a client of Van Gaalen's). In the e-mail message itself Van Gaalen stated that Wright was unreliable and not to be trusted. Van Gaalen also attached an e-mail from Wright to Van Gaalen, in which Wright had appeared to indicate that he was overcharging Ablaze. This had damaged the relationship between Wright and Ablaze, and Wright had claimed in defamation against Van Gaalen.

Van Gaalen first testified that he had not intended to address the e-mail to Williams but rather to Brown; however, because the e-mail was about Williams "he must have mistaken the first letter of Mr. Williams' address for that of Mr. Brown's as a result of his 'hunt and peck' style of typing" and Williams' name had been pulled up from his e-mail program's contact list. In cross-examination Van Gaalen stated that, in fact, he had intended initially to send the e-mail to Williams, but then changed his mind and tried to send it to Brown, inadvertently sending it to Williams instead. Brown had never received the e-mail.

Schultes J. first found that the words used in the e-mail were clearly defamatory in their ordinary sense, and thus would have been defamatory whether or not they had been sent to Brown or Williams. Van Gaalen's counsel argued that the words did not amount to defamation because it was Wright's own statements (in the attached e-mail) which damaged the relationship between Wright and Williams. Justice Schultes ruled:

> Obviously, merely forwarding one's own comments in an email cannot in itself amount to defamation—it must be found in something actually written by the person who forwarded it. However,… the question of what harm actually flowed from the email, in terms of Mr. Williams' withdrawal of his business, goes to the issue of damages, not whether what was written by Mr. Van Gaalen was defamatory. If, as I have found, the words he wrote are defamatory to an ordinary reader, it does not matter on the issue of liability what Mr. Williams, the specific intended recipient, made of the entire email (paras. 112-113).

As a result, damages in defamation were ordered.

Service via E-mail... to Mobile Device

In *Holland v. Holland*, Justice J.B. Veit of the Alberta Court of Queen's Bench heard a special chambers motion by the plaintiff to finalize the dissolution of her marriage, including the settling of divorce, custody, child support, a restraining order and dividing matrimonial property. The plaintiff had earlier applied for and received an order permitting her to serve the defendant via e-mail, though as Justice Veit noted, "at the time of granting of the order relating to service, the court was not aware of the amount of material that Ms. Holland would be required to serve on her husband" (para. 1). While she did not file an affidavit of service, the plaintiff indicated through her counsel that she had forwarded a number of e-mails with attached documents to the defendant. There was no evidence that the defendant had a computer at the relevant time, though there was some evidence that he had paid for service from Koodo, "and it may be that Koodo is a mobile telecommunications provider" (para. 30).

Regarding the service issue, Justice Veit began by noting that service via e-mail, "as anticipated in the New [Alberta Civil Procedure] Rules, is undoubtedly a great step forward in facilitating access to justice" (para. 32). However, she viewed it as necessary that where a party to litigation only has access to a mobile receiving unit as a means of receiving e-mail or other electronic communications, it was imperative that other parties indicate this in the affidavit supporting any application for substituted service. This was so the court could determine whether service via e-mail was, in fact, appropriate in such a circumstance. She then provided some detail regarding the kinds of concerns the court may have:

> The size of scanned documents, whether they be attached or embedded into email, present challenges. Most email systems have size limitations, sometimes as low as 20MB, that would prevent an email recipient from receiving anything that exceeds that limitation. Determining a safe number of scanned documents, or size of a single document, which can be transferred is also difficult because the format the document is saved in has a direct impact on how big the file will be for a given document. In general terms, a document which is prepared, for example, in Word or WordPerfect format is likely to have a fairly small footprint - maybe even less than 1MB - but scanned documents have a fairly large footprint.
>
> Also, since the server/software that services mobile devices is typically separate from the email system software/servers, there is no built-in ability to receive a status report from the mobile device back to the sender. Not only do not all email systems send back status indications to the senders that an email has been received, some email systems may allow the receiver to determine if they want to allow such a status message to go back to the sender. This is different from the ordinary mail system where, as we have seen in this case, a sender often receives notification that the intended receiver no longer resides at the stated address (paras. 33-34).

In the end, there was no evidence that the defendant had received notice of the proceeding, nor specifically that he had received all of the documents sent to him, and no basis for assuming so. While the various orders applied for were granted in some form, Justice Veit held that the defendant could not be held in breach of any of them until there was evidence that he was personally served with the decision and order. Moreover, the order permitting service via e-mail was quashed and the plaintiff was required to make a new application for substituted service.

Banned in France: Google and Twitter

It was recently reported that, on 27 May 2011, the Superior Audiovisual Council (CSA) of France ruled that television and radio broadcasters could not direct their listeners/viewers to their Facebook or Twitter sites, but could only reference generic social media. "Plugging" a broadcaster via these particular sites was deemed to be in violation of a 1992 law which prohibits "secret advertising" on radio and television, i.e. broadcasting the logos or names of third party companies which had not paid for the service. The ruling and law were justified by a CSA

representative on the basis that, in France, companies did not have to pay for access to the airwaves and thus had to follow more restrictive rules. Initial reaction was critical.

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.

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.