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

November 30, 2011

IT.Can NEWSLETTER

Canadian IT Law Association

www.it-can.ca

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

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

Privacy Commissioners Criticize Lawful Access Legislation

Both the Privacy Commissioner of Canada, Jennifer Stoddart, and the Information and Privacy Commissioner of Ontario, Ann Cavoukian, have recently and publicly criticized the federal government for its intention to re-introduce its "lawful access" electronic surveillance bills (C-50, C-51 and C-52). On 26 October 2011 Commissioner Stoddart sent an open letter to Public Safety Minister Vic Toews, expressing her "deep concern" that, despite the government's "firm and repeated commitments to the importance of privacy," they were proposing to enact legislation that would drastically increase the state's surveillance and scrutiny powers, while at the same time weakening judicial scrutiny of the use of these tools. No evidence had been provided, she argued, that such new powers were needed for the government to carry out its legislative mandate, nor had justification been presented for their breadth. There was no demonstration that the route was the least privacy-invasive possible, nor any proof of legal proportionality or practical effectiveness. She also expressed concern about "the adoption of lower thresholds for obtaining personal information from commercial enterprises:"

> The new powers envisaged are not limited to specific, serious offences or urgent or exceptional situations. In the case of access to subscriber data, there is not even a requirement for the commission of a crime to justify access to personal information – real names, home address, unlisted numbers, email addresses, IP addresses and much more – without a warrant. Only prior court authorization provides the rigorous privacy protection Canadians expect.

Commissioner Cavoukian's letter, addressed to both Minister Toews and Justice Minister Rob Nicholson, expressed her support for Commissioner Stoddart's letter, but offered a detailed, five-point analysis of why, in her view, re-introducing the bills unchanged "would be highly regrettable for the people of Ontario and Canada." The Commissioner summarized her argument as follows:

1. The proposed powers must not come at the expense of the necessary privacy safeguards guaranteed under the *Canadian Charter of Rights and Freedoms*; in order to maintain the integrity of this constitutional framework, the government must acknowledge the sensitivity of traffic data, stored data, and tracking data.

2. Intrusive proposals require essential matching legislative safeguards; the courts, affected individuals, future Parliaments, and the public must be well informed about the scope, effectiveness, and deleterious effects of intrusive powers. If Parliament enacts expansive new surveillance powers, we urge the federal government to publicly commit to enacting the necessary oversight legislation in tandem.

3. Even with matching oversight, the proposed surveillance and access powers will require more stringent conditions precedent to determine the situations when surveillance or access may be appropriate and necessary.

4. The government must not impose a mandatory surveillance capacity regime on the public and its telecommunication service providers (TSPs) without adequate safeguards to protect the future of freedom and privacy; a comprehensive and public cost-benefit analysis should precede rather than follow the making

of so many significant public policy decisions. Public Parliamentary hearings should be scheduled to ensure that civil society, as well as industry, have a full opportunity to provide substantial input on all of the Bills including Bill C-52 (the *Electronic Communications Act*). In addition, the *Electronic Communications Act* should be amended to require that all interception-related capacity requirements be approved by Parliament before they can be imposed.

5. The proposal for warrantless access to subscriber information is untenable and should be withdrawn; it remains our view that the *Electronic Communications Act* should be amended to require that the provisions setting out TSP obligations concerning "subscriber information" be deleted and replaced with a court supervised regime

Internet Defamation: IOC Should Be Sued in Switzerland

In *Elfarnawani v. International Olympic Committee*, Justice Kenneth Campbell of the Ontario Superior Court of Justice heard a motion requesting the court to decline jurisdiction over an action brought for, *inter alia*, internet defamation. The plaintiff, who had previously had involvement with the Lausanne, Switzerland-based International Olympic Committee (IOC) had been implicated in a BBC TV investigative journalism report, during the course of which he spoke with undercover reporters. In the television footage he suggested that he could be retained by parties who sought the locating of the Olympic Games in a particular city and, for a fee, essentially buy votes from members of the IOC, as well as that he had access to confidential decisions made by the IOC. The Ethics Commission of the IOC recommended that he be declared *persona non grata* in the Olympic Movement and to encourage all affiliated organizations not to have any dealings with him. The Executive Committee of the IOC carried out the recommendation, and all of this was communicated to the public via the IOC website. The plaintiff sued the IOC in Ontario for defamation, breach of a duty of good faith and abuse of process. The IOC moved to dismiss the action on the basis that Ontario did not have jurisdiction over it, or alternatively that Ontario was *forum non conveniens*.

The plaintiff argued that his action fell under Ontario Civil Procedure Rule 17.02(g), which presumes a real and substantial connection over "torts committed in Ontario," and Justice Campbell embarked on determining whether the allegedly tortious conduct had taken place in Ontario. Citing past jurisprudence, including the Supreme Court of Canada's recent decision in Crookes v. Newton, Campbell J. noted that any potential internet defamation could only have occurred in Ontario if the remarks in question were published in Ontario, which required proof that someone besides the plaintiff or his agents actually accessed the information. Publication could also occur, he noted, in any location which appeared to have been "targeted" by the posting of the material. He remarked:

> The internet undoubtedly provides a powerful vehicle for defamatory expression, and has an extraordinary capacity to harm an individual's reputation. See: *Barrick Gold Corp. v. Lopehandia* 2004 CanLII 12938 (ON CA), (2004), 71 O.R. (3d) 416 (C.A.), at para. 32; *Crookes v. Newton*, at para. 37. It is important to recall, however, that this unprecedented accessibility of information through the internet does not itself establish that any specific piece of posted information has actually been viewed by anyone. While there are surely popular websites that are visited millions of times daily by interested individuals around the globe, it is equally true that there are countless websites that are accessible worldwide but which are of no interest to anyone but the site's own creator and webmaster. Clearly, not every internet website can boast the popularity of Google or Facebook. Nor does convenient world-wide accessibility, regardless of the popularity of the individual website, obviate the legal requirement for "publication" of any alleged defamation. In other words, in internet defamation cases the plaintiff must still establish that the allegedly defamatory material was actually viewed by some independent third party (ie. someone other than the plaintiff and/or his or her legal representative) (para. 32)

In this case there was no evidence that anyone except the plaintiff had viewed the material, nor any evidence that the IOC website had targeted Ontario. No presumptions or fact-finding via judicial notice were available; "the issue of 'publication' is a matter of proof, by evidence, in each individual case" (para. 34). Moreover, the IOC's website strictly passive in terms of directing the content and there was no evidence that any jurisdiction in particular had been targeted.

Justice Campbell also rejected the plaintiff's further argument that there was a "real and substantial connection" of the matter to Ontario. The IOC itself, despite the website's international reach, had no particular connection to Ontario. While any damage suffered by the plaintiff would likely have been in Ontario, there was no evidence of such. Accordingly, jurisdiction simpliciter had not been established. In considering the issue of *forum non conveniens* in the event he had erred in his earlier findings, the court observed in part that a tab marked "Legal Information" on the IOC website indicated that any disputes regarding content of the site were solely within the jurisdiction of the Lausanne-based Court of Arbitration for Sport. To the extent this was applicable to the plaintiff's claim, "this 'agreement' suggests that Switzerland is the convenient forum for the resolution of any dispute between the parties" (para. 64). The action was ordered dismissed.

Cell Phones and Search Incident to Arrest

The continuing issue of the extent to which an electronic storage device (such as a smart phone) can be searched incident to arrest arose once again in *R. v. Hiscoe* (no hyperlink available). The accused was arrested after being observed, while under surveillance, to pass an item to the driver of another vehicle which he had met at an empty drive-in movie theatre. The arresting officer seized the accused smart phone and made a cursory examination of the test messages on it at the time. Later that evening the officer re-examined the smart phone in order to record in writing those text messages. Finally, one month later the police sent the phone to the RCMP Forensic Crime Lab and the complete contents of the phone's data was downloaded (referred to in the case as the "data dump"). The accused argued that all three searches – the examination at the scene, the transcription later that day, and the data dump – violated his right under section 8 to be free from unreasonable search and seizure. The Crown argued that all three searches were authorized by law as part of a search incident to arrest.

The trial judge ultimately concluded that the examination at the scene and the later transcription were part of a valid search incident to arrest, but that the data dump was not. Accordingly he found that evidence to have been unlawfully obtained and excluded it under section 24(2).

The decision engages in a very complete discussion of Canadian and US case law on the subject of searches of electronic storage devices, particularly as part of a search incident to arrest. Judge Tufts begins with the leading Supreme Court of Canada cases on search incident to arrest (which do permit searching for evidence of the offence as a legitimate purpose) but notes that:

> The difficulty with the jurisprudence in this area of the law is that devices which contain such vast amounts of personal information were never contemplated, even a decade ago, to be carried on individuals. (para 83)

He observes that a search incident to arrest is not open-ended, and that the purpose of the search must be related to the arrest. In the case of a search for a physical object, it is relatively easy to explain why it would be reasonable (or not) to search a particular location. The same built-in limitation does not exist in the case of information on a smart phone, and therefore, he finds, the search power must be limited in some way. He observes:

> 78 ... it was never contemplated that the reference to the discovery of evidence as a valid objective for justifying search upon arrest would include a justification to conduct a full investigation style search. The focus was, in this regard, to search to preserve evidence present at the arrest scene. A cell phone, in a way is a portal into the personal lives of an arrestee beyond what is related to the reasons for the arrest...

A smart phone cannot be compared with a notebook or briefcase, which an accused might have for a particular purpose. Rather "these types of devices

allow individuals to carry their entire personal information library with them" (para 43). Further, he notes that cell phones are organized in a way that separates voice messages, text messages, documents, photographs, browser history and other information. Accordingly it is possible to look at one type of information without the need to look at everything else.

Because the accused had been arrested while delivering drugs, it was reasonable to think he might have just arranged that rendezvous using his smart phone, and so checking the text messages at the scene was part of a search incident to the arrest. Similarly transcribing the text messages later that day was still incident to the arrest. (The judge observed that the arresting officer has testified that there was technology which permitted the deletion of text messages from a remote location: this was simply an assertion from the officer, but since it was unchallenged Judge Tufts accepted it as true for purposes of the hearing.)

The data dump, however, was not part of the search incident to arrest. It was not conducted until a month later, was an examination for information rather than for the physical characteristics of the phone, and most importantly was too broad to be incident to the arrest. No attempt was made to tailor the search to the particular parts of the smart phone where there was a reasonable prospect of discovering evidence. Further, downloading the digital files completely compromised the accused's privacy interests in a way that looking in a briefcase or glancing into a family album would not. If the police did want to conduct such a search, the judge held, the proper course was to seek a warrant, which could be properly limited.

Cell Phones and Email

An evidentiary point around email arose in *R. v. Beteta-Amaya* (no hyperlink available) in which the accused was charged with making a false report to the police. He had reported that his ex-girlfriend and his new partner (who were bound by recognizances to stay away from him) had accosted him on the street and threatened him. The ex-girlfriend and her partner persuaded the police (and ultimately the trial judge) that they had been elsewhere at the time of the alleged incident: part of that evidence was an email sent by the ex-girlfriend during the time she was supposed to be accosting him. She reported that she had sent that from a computer in a building some distance away.

The accused argued that she could have sent the email from her cell phone, and therefore that this evidence did not establish that she was elsewhere. The trial judge accepted the explanation that if she had sent it from her cell phone it would have contained a notation such as "Sent from Blackberry", or "Sent from Iphone", which the email did not have. The trial judge also accepted that emails sent from her cell phone had a different personalized signature than the one which appeared in the email.

Access to Information and the CBC

In *Canadian Broadcasting Corporation v. Canada (Information Commissioner)* the Federal Court of Appeal has concluded that the CBC is required to turn over records to the Information Commissioner when it has refused to disclose those records in response to an access to information request and the refusal is challenged. The only exception to this result is when the request concerns information regarding a journalistic source.

The CBC has been subject to the *Access to Information Act* since 2007, and had received nearly 1000 requests for information when this action was commenced. Some information is exempt from the application of the Act under section 68.1, specifically information that relates to its journalistic, creative or programming activities. However, that exemption is itself subject to an exception: "other than information that relates to its general administration." The CBC had refused to release information in response to various requests on the generic basis that it related to journalistic, creative or programming activities. In some cases those refusals were the subject of complaints to the Information Commissioner. In the course of deciding complaints, the Commissioner has the authority under section 36(2) to "examine any record to which this Act applies."

The Commissioner's position was that she was entitled under section 36(2) to see the records which the CBC refused to disclose, in order to decide whether the refusal was justified. The CBC took the

view that because the requests in issue concerned journalistic, creative or programming activities, they were *not* records to which the Act applied and so the Commissioner had no power to examine them.

The Federal Court Trial Division had sided with the Commissioner on the interpretation of the Act, and the Federal Court of Appeal upheld that decision. The CBC's view, they observed, would make the CBC both a party in the cause and the judge in a dispute. Further, they noted, the exception in section 68.1 was phrased to recognise that some records could be part of journalistic, creative or programming activities *and* relate to general administration: in that event the argument that the records fell outside the Act was incorrect. Further they noted that the exemption applied to "information" contained within records, not to the records themselves, and so the CBC could not simply refuse to release the entire document. They also observed that the practice which had been adopted by the CBC of refusing to release on the generic ground was improper: they were required to say which of the three exemptions was meant to apply.

The Federal Court of Appeal did agree, however, that journalist-source privilege was to be respected. Although the Commissioner was meant to have access to records generally to fulfill her role of deciding whether an exemption applied, a request seeking the disclosure of a journalistic source could not fall within the exception and so a record revealing that type of information would be exempt from the Commissioner's power of examination.

Facebook Settles Privacy Charges With FTC

Facebook, which has been charged by the US Federal Trade Commission for misleading its users regarding the use and sharing of their private information, beyond the privacy settings available to them, has entered into a settlement agreement. In it, Facebook agrees to provide clear and prominent notice to users regarding the use of their information. The text of the agreement can be found here.

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 Professor Robert Currie, Director of the Law & Technology Institute, at robert.currie@dal.ca.

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 le professeur Robert Currie à l'adresse suivante : robert.currie@dal.ca