Blaney McMurtry LLP

PUBLICATION

So you think your information is safe on Google Drive…

Date: November 01, 2018

Original Newsletter(s) this article was published in: Commercial Litigation Update: November 2018

"If you want to keep a secret, you must also hide it from yourself" - George Orwell, 1984

It comes as no surprise that sweeping technological advances in the past decade have changed the way Canadians do business. As a result, commercial litigators now know that when disputes arise, a good portion of the relevant evidence will be in electronic form. Paper is increasingly on its way out of most businesses, replaced by employee laptops and tablets, smartphones, servers, and cloud storage.

According to the *Rules of Civil Procedure* all documents relevant to the issues in dispute in a parties' possession or control must be produced to the other side as part of the "discovery" (i.e. disclosure) process. In a world where damaging documents or emails can be deleted in the blink of an eye, hard-drives can be scrubbed, and passwords and encryption keys can be withheld or conveniently "forgotten", lawyers often face an uphill battle in obtaining the preservation and disclosure of such documents and information from the opposition.

What weapons does the commercial litigator have in her arsenal to prevent her client's opponents from destroying critical electronic data that may prove harmful to their case in court? Only a select few. The law of Canada includes the tort of "spoliation", i.e. the intentional tampering or destruction of evidence. However, the remedy simply raises the rebuttable presumption that the spoliated evidence would not have favoured the party who tampered with or destroyed the evidence. In other words, while an adverse inference may be useful, spoliation does nothing to help the other party actually obtain or preserve the evidence, as spoliation presumes that the evidence is already gone.

To actually preserve and obtain electronic evidence, one has to get a bit more creative. Blaneys' commercial litigation team has recently been involved in a spate of cases dealing with precisely this issue and may have "cracked the code".

In what is believed to be the first such instance of its kind, Blaneys successfully brought an *ex parte* (meaning “without notice”) motion for the preservation of electronic data based on Rule 45 of the *Rules of Civil Procedure* to preserve the contents of an opponent’s personal Google Drive and iPhone.

Rule 45 provides that “the court may make an interim order for the custody or preservation of any property in question in a proceeding or relevant to an issue in a proceeding, and for that purpose may authorize entry on or into any property in the possession of a party or of a person not a party”. Rule 45 clearly contemplates the preservation of physical, tangible property, but in Blaneys’ case, the property to be preserved was data contained in Google Drive cloud storage and text messages on an iPhone. Blaneys thus had to re-fashion Rule 45 to suit its client’s needs.

The plaintiff sued the defendant company, represented by Blaneys, for damages arising from the alleged wrongful termination of a consulting services agreement. The defendant counterclaimed for damages resulting from the plaintiff’s misappropriation of confidential information and customers in breach of a non-competition covenant.

Numerous demands were made on the plaintiff for the return of a laptop belonging to the defendant. Ultimately, the plaintiff relented and delivered the laptop to Blaneys’ offices, but upon inspection by a forensic expert, it was discovered that the plaintiff had deleted all of the data on the laptop by reformatting the laptop and reinstalling the operating system.

The plaintiff also sent the defendant a USB key containing a handful of confidential documents confirmed by Blaneys’ forensic expert to have come from the plaintiff’s personal Google Drive (cloud storage) account. It therefore appeared that the plaintiff had backed up some or all of the laptop’s contents onto his Google Drive account before scrubbing the laptop and sending it to Blaneys. The plaintiff must not have counted on the USB key being scrutinized to this extent (or was unfamiliar with the long-reach of digital forensic examiners).

Blaneys immediately contacted Google LLC and requested that it record the contents of the plaintiff’s Google Drive by taking a “snapshot” of the Google Drive. Google agreed to do so, but for a limited period of time only. It was therefore important that Blaneys bring the motion for a court order securing the further preservation of the data in the Google Drive account without delay.

The plaintiff had also used his personal iPhone to send text messages for company business. As a result, the motion was brought for the preservation of the contents of both the Google Drive *and* the iPhone, for all information dating back to the material time.

Since the evidence established that the plaintiff had already deleted key evidence once (i.e. by reformatting the laptop) Justice Nakatsuru was persuaded to grant the defendant an *ex parte* preservation order for the data on the plaintiff’s Google Drive and iPhone relevant to the issues in the litigation, which is to remain in effect until the disposition of the action. Specifically, Justice Nakatsuru found that because the plaintiff had taken steps to delete and reformat the

company's laptop in the face of direct and persistent demands for its return in a preserved state, there was a "juridical basis" to conclude that giving notice to the plaintiff could defeat the motion and therefore would not be in the interests of justice.

This case highlights the difficulties faced by Ontario law to maintain its effectiveness in the face of a rapidly changing business and litigation landscape. It is often said that the *Rules* need an update to reflect commercial realities and, in particular, the pervasive use of technology in today's world. But until then, parties will have to rely on creative lawyering and forward-thinking judges to ensure that evidence is treated fairly and parties are not prejudiced as a result of the speed with which key electronic data can be forever lost.