Shelley Jones and Robert MacDonald here consider the recent decision of Google Inc. v. Equustek Solutions Inc. at the Supreme Court of Canada by looking at the background of the case, the challenges that arose, and the repercussions of the decision.

As Canadians celebrate 150 years as a nation in 2017, a decision of the Supreme Court of Canada in Google Inc. v. Equustek Solutions Inc. has generated some fireworks of its own. In granting an interlocutory injunction requiring Google to de-index websites on a global basis, this case has implications for intellectual property (IP) rights holders’ enforcement strategies both in Canada and abroad. The case also illustrates the particular challenges, including jurisdictional challenges, involved when seeking to protect IP rights in the online environment. In an added twist, the United States District Court (Northern District of California) recently stepped in and granted Google’s motion for a preliminary injunction to prevent the enforcement of the Canadian order.

**Case background**

The case stems from a dispute between Equustek Solutions Inc. ("ESI") and Datalink Technologies Gateway Inc. ("Datalink"). ESI is a Canadian company that designs, manufactures, and sells industrial network interface hardware that enables communications between complex industrial equipment. ESI alleged that, in addition to trademark infringement though re-labelling ESI’s product and passing it off as its own, Datalink unlawfully obtained confidential information and trade secrets belonging to ESI. Datalink then used this information
to create and sell a competing product, the "GW1000".\(^5\)

When ESI commenced the action in 2011, Datalink, a former distributor of ESI's, was also based in Canada. However, when Datalink stopped responding to communications in the litigation and refused to comply with court orders, it became apparent that it had moved operations outside of Canada. In the type of scenario all too familiar to many IP owners seeking to enforce rights against internet infringers, a proverbial game of cat and mouse with Datalink ensued. Datalink continued to carry on business using a variety of websites, filling orders from unspecified locations, and changing periodically in order to operate in a "clandestine" manner.\(^6\) In spite of their investigative efforts, ESI was ultimately unsuccessful in tracking down and enforcing the court orders previously obtained against Datalink. This included an order in December 2012 prohibiting Datalink from carrying on business through any website.\(^7\)

Frustrated that, despite the court orders, Datalink was still selling the infringing product and customers were locating Datalink's websites via online searches, ESI then sought to have Google Inc. ("Google") de-index certain webpages associated with Datalink from its search results. Google responded by voluntarily de-indexing 345 webpages from its Canadian search engine site at <google.ca>. According to ESI, this approach was unsatisfactory because new websites would automatically move up in the rankings to take the place of previous sites. Datalink was also relocating content within their websites to circumvent the blocking of certain web pages.\(^8\) In an effort to block entire domains and extend the de-indexing worldwide via <google.com>, ESI subsequently obtained an interlocutory injunction from the Supreme Court of British Columbia ordering Google to globally de-index Datalink's websites. In granting the order, the court held that it had territorial competence. The court also held that it had authority to make the order against Google, a non-party to the proceedings and resident in a foreign jurisdiction. In granting the order, the court acknowledged the inherent challenges encountered by parties attempting to enforce their rights online:

"The Court must adapt to the reality of e-commerce with its potential for abuse by those who would take the property of others and sell it through the borderless electronic web of the internet.\(^9\)"

An appeal by Google to the Court of Appeal was subsequently dismissed. In a unanimous decision, the Appeal judges affirmed the lower court's ruling that it had territorial competence and the injunction did not violate principles of comity. The Court of Appeal also found that the order did not violate any freedom of speech norms.\(^10\) This decision was further appealed to the Supreme Court of Canada.

In a decision issued in June 2017, the Supreme Court of Canada affirmed both rulings of the lower courts and upheld the worldwide interlocutory injunction against Google. In a 7-2 split, the
majority held that a worldwide injunction was the "only effective way to mitigate the harm to ESI pending the trial":

“Datalink and its representatives have ignored all previous court orders made against them, have left British Columbia, and continue to operate their business from unknown locations outside Canada. Equustek has made efforts to locate Datalink with limited success. Datalink is only able to survive - at the expense of Equustek's survival - on Google's search engine which directs potential customers to its websites. In other words, Google is how Datalink has been able to continue harming Equustek in defiance of several court orders.

This does not make Google liable for this harm. It does, however, make Google the determinative player in allowing the harm to occur. On balance, therefore, since the interlocutory injunction is the only effective way to mitigate the harm to Equustek pending the resolution of the underlying litigation, the only way, in fact, to preserve Equustek itself pending the resolution of the underlying litigation, and since any countervailing harm to Google is minimal to non-existent, the interlocutory injunction should be upheld.\(^{11}\)

However, the minority favored judicial restraint. In the dissenting opinion, the effectiveness of the injunction was questioned on the basis that it required ongoing modification and supervision due to Datalink's tactics of replacing de-listed websites with new ones. Moreover, Datalink's websites could still be located "...using other search engines, links from other sites, bookmarks, email, social media, printed material, word-of-mouth, or other indirect means" and Datalink's "...websites are open for business on the Internet whether Google searches list them or not"\(^{12}\). The dissenting view also raises the issue of other enforcement options available to ESI including pursuing a remedy in the French courts, (where the proposed defendants resided and had assets) seeking injunctive relief against the ISP providers, or commencing contempt proceedings in jurisdictions where there may have been links to Datalink's various websites.\(^{13}\)

**Challenges in online enforcement of IP rights**

The Equustek decision and the facts of the case highlight the challenges in enforcing IP rights on the internet, where counterfeiting and piracy activities abound. A 2016 report published by the Organization for Economic Cooperation and Development (OECD) and the European Union Intellectual Property Office (EUIPO) titled "Trade in Counterfeit and Pirated Goods: Mapping the Economic Impact" outlines the inherent difficulties in dealing with counterfeit trading online:
Building on the OECD/EUIPO report, a recent Frontier Economics paper was commissioned by the International Trademark Association (INTA) and the International Chamber of Commerce (ICC) Business Action to Stop Counterfeiting and Piracy (BASCAP) initiative. The report, entitled *The Economic Impacts of Counterfeiting and Piracy*, estimates that the global trade in illicit goods will reach US$991 billion by 2022.

The internet will continue to play a significant role in facilitating such growth as new technologies and platforms offering opportunities to simultaneously increase sales while avoiding enforcement. For example, the expansion of generic Top-Level Domains (gTLDs) is expected to contribute to online piracy and trading in counterfeit goods. As of July 31, 2017, of the total 1,930 applications submitted, 1,227 new gTLDs have been delegated so far. This is expected to contribute to increased "domain name hopping", a process that involves changing domain names as well as masking their locations and using servers in various jurisdictions to evade enforcement efforts.

Social media is also proving to be a major conduit for the sale of counterfeit and pirated goods. According to a report from the U.K. National Trading Standards, eCrime Team, "...social media has overtaken auction sites as criminals' 'channel-of-choice' for counterfeiting and piracy activity". The U.K. report was cited in the comprehensive 2017-2019 Joint Strategic Plan on Intellectual Property Enforcement released by the Office of the U.S. Intellectual Property Enforcement Coordinator (IPEC) in December 2016. The misuse of social media channels to promote infringing activity is listed in the Plan as an issue requiring action including, for example, "...the development of industry standards and best practices, through a multistakeholder process".

In addition, IP owners are dealing with the emergence of the "Dark Web", an area of the internet where cybercrime flourishes. Recent cases involving "darknet" internet marketplaces reveal the extent of the problem as well as its international implications. In July 2017, two of the largest dark web markets, AlphaBay and Hansa, were taken down as a result of an operation...
by the FBI, the U.S. Drug Enforcement Agency (DEA) and Dutch national police with cooperation from Europol, the Royal Canadian Mounted Police and other law enforcement agencies.\textsuperscript{20} According to law enforcement, an estimated $1 billion in trades using digital currencies were made via AlphaBay since its launch in 2014.\textsuperscript{21}

A key means of disrupting counterfeiting and online piracy usually involves tracking the flow of money but, as with most internet-related issues, this is not an easy task give the current global financial system.\textsuperscript{22} According to the recent U.S. Joint Strategic Plan:

"This includes an examination of a "follow-the-money" approach to disrupt illicit financing models (via payment processors, ad networks and the like), to practices and policies aimed at curbing abusive practices within e-commerce platforms, social media channels, the domain name ecosystem, and the search environment, among others.\textsuperscript{23}"

The Plan's recommendations also involve strengthening international banking practices and encouraging participation from third party financial technology processors.\textsuperscript{24} The Canada Anti-Fraud Centre (CAFC) (operated under the Royal Canadian Mounted Police) has developed an effective program called "Project Chargeback", which adopts a unique "follow the money" approach, with Canada being the first country to introduce this model.\textsuperscript{25} The Chargeback Program began in 2012 with the CAFC working together with credit card companies and banks to provide reimbursement to those who have fallen victim to sellers of counterfeit goods online and can result in shutting down the counterfeit retailer's accounts.\textsuperscript{26} As of March 2017, 35,000 chargebacks have been issued with over $10 million recovered.\textsuperscript{27} The CAFC approach represents the kind of multistakeholder model that can offer a low cost and effective means of deterring online infringement.

**Canadian order enjoined in the US**

Having been unsuccessful before the Supreme Court of Canada, Google turned to the US courts for assistance and brought an action in the US District Court to prevent the enforcement of the Canadian order. It then moved for a preliminary injunction. ESI did not file an opposition brief but apparently it did write to the court saying that it did not intend to defend the action. It also said that it thought the motion was "unnecessary and unfair".\textsuperscript{28}

In the action, Google seeks a declaratory injunction that the Canadian order cannot be enforced in the United States and an order preventing enforcement of the Canadian order on the basis that it:

1. Directly conflicts with the First Amendment of the United States Constitution;
2. Disregards the immunity for interactive service providers under the United States Communications Decency Act; and,
3. Violates principles of international comity.\textsuperscript{29}

The court hearing the application for the preliminary injunction focused on the issues raised under the Communications Decency Act and did not address the other issues raised by Google.

The purpose of Section 203 of the Communications Decency Act was summarized by the court:

\begin{quote}
"Section 230 of the Communications Decency Act "immunizes providers of interactive computer services against liability arising from content created by third parties." Fair Hous. Council of San Fernando Valley v. Roommates.com, ..... It states that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." ..... Congress enacted Section 230 in 1996 to address "the threat that tort-based lawsuits pose to freedom of speech in the new and burgeoning Internet medium." Zeran v. Am. Online, Inc., .....\textsuperscript{30}\"
\end{quote}

The court was satisfied that Google was entitled to the protection of Section 203:

1. Google is a provider of an interactive computer service;
2. The information in question was provided by another information content provider, namely Datalink. The court held that "Datalink - not Google - 'provides' the information at issue. Google crawls third-party websites and adds them to its index; When a user queries Google's search engine, Google responds with links to relevant websites and short snippets of their contents; Google's search engine helps users discover and access content on third-party websites, but it does not "provide" that content within the meaning of Section 230\textsuperscript{31};
3. The Canadian order would hold Google liable as the "publisher or speaker" of the information on Datalink's websites. "The Supreme Court of Canada ordered Google to 'de-index the Datalink websites' from its global search results because, in the Court's view, Google is 'the determinative player in allowing the harm to occur' to Equustek. ..... The Ninth Circuit has held that, regardless of the underlying cause of action, a claim treats an intermediary as a publisher when it requires the intermediary to remove third-party content. ..... 'Removing content is something publishers do, and to impose liability on the basis of such conduct necessarily involves treating the liable party as a publisher of the content it failed to remove.' ..... The Canadian order treats Google as a publisher because the order would impose liability for failing to remove third-party content from its search results."\textsuperscript{32}

Accordingly, the court concluded that Google was harmed by the Canadian order because it
would restrict activity that Section 203 protects. Further, the court was satisfied that granting in
the preliminary injunction would serve the public interest. As a result, a preliminary injunction
was granted.

**Conclusion**

As IP infringers continue to leverage existing and new technologies, law enforcement,
governments, and rights holders find it challenging to keep pace. For most IP owners, as
reflected in the comments by the dissenting judges in the Supreme Court of Canada decision in
Equustek, obtaining court orders for de-indexing may only get you so far. The underlying
problem of domain name hopping and circumventing enforcement still remains. Although de-
indexing may be an effective tool for disrupting an infringer's sales, it ultimately represents only
one piece of the "whack-a-mole" game that IP owners often face and, as demonstrated by the
preliminary injunction in the US, raises serious jurisdictional issues. Consequently, effective IP
enforcement in the online space requires a multi-pronged approach along with cooperation
amongst the many government, business, law enforcement, policy and other key stakeholders
involved.

**Résumés**

**Shelley Jones**

Shelley is a Lawyer and Registered Trademark Agent based in Ottawa. She is a Fellow of the
Intellectual Property Institute of Canada (IPIC) and a member of IPIC's Anti-Counterfeiting
Committee. Shelley is also a member of the International Trademark Association (INTA) and
serves on the INTA In-House Practitioners Committee.

**Robert MacDonald**

Robert was called to the Ontario Bar in 1983 and is a Registered Trademark Agent practicing
with Gowling WLG with a focus on prosecution, oppositions and litigation in the Federal Court.
He is recognized as a leading trademark practitioner by various publications including WTR1000
and by Chambers Global.

---

1 Google Inc. v. Equustek Solutions Inc., 2017 SCC 34.

3 Google Inc. v. Equustek Solutions Inc., supra at para. 3 (SCC).


7 Equustek Solutions Inc. v. Datalink Technologies Gateways LLC, supra, para. 7 (BCSC).


9 Equustek Solutions Inc. v. Datalink Technologies Gateways LLC, supra, para. 159 (BCSC).

10 Equustek Solutions Inc. v. Google Inc., supra, para. 5 (BCCA).

11 Google Inc. v. Equustek Solutions Inc., supra, at paras. 52 and 52 (SCC).


17 USTR (2015), 2014 Out-of-Cycle Review of Notorious Markets, at page 15: In a comment on Kickass Torrents, the USTR noted that "...over the past several years the site operators have changed the domain name numerous times, obscured or hidden their locations, and have used multiple servers in various countries to evade or otherwise frustrate enforcement action."


Trademarks and Brands Online, "Dark web counterfeit hubs shut down" (July 24, 2017). See: http://www.trademarksandbrandsonline.com/news/dark-web-counterfeit-hubs-shut-down-5042; see also:


The Register, "Cops harpoon two dark net whales in megabust: AlphaBay and Hansa", John Leyden (July 20, 2017). See: https://www.theregister.co.uk/2017/07/20/dark_net_megabust/


Google LLC v. Equustek Solutions Inc., supra, pages 4-5.

This article was first published in the Trademark Lawyer Magazine.