Focus
INTELLECTUAL PROPERTY

Trade dress for success

Marlboro decision defeats marketing tactic of look-alike brand

LUIGI BENETTON

Philip Morris owns the trademark for Marlboro, the top-selling international cigarette brand, in most of the world. But not in Canada.

Thanks to that quirk — the result of a long-ago trademark sale by a Philip Morris predecessor company to what is now Imperial Tobacco — Philip Morris tried a new marketing tactic in 2006. They marketed a brand using the red-and-white ("red roof") Marlboro packaging trade dress, without a name on the package.

Trade dress refers to visual characteristics of a product or its packaging that serve to identify it for consumers.

"They used the trademark 'Matador' before that," says Brian Gray, senior partner with Norton Rose Fulbright Canada.

Here's another twist: in Canada, retailers must keep cigarettes behind store counters and conceal the shelves that hold them, which results in a "dark" market. So instead of picking a carton off a shelf, consumers must ask for a brand, which raises the question: how do you ask for a brand that doesn't display its name on the packaging?

Imperial Tobacco successfully raised that very question in court during *Philip Morris Products S.A. v. Marlboro Canada Limited* [2012] F.C.J. No. 878. The Supreme Court later denied Philip Morris leave to appeal Imperial's earlier trademark victory.

Other factors contribute to the unique nature of this case. For instance, the red rooftop design flows over borders. Even when cigarette advertising was prohibited at the Canadian Grand Prix, Ferraris sped around Montréal's Circuit Gilles-Villeneuve sporting the red rooftop on their rear spoilers. Even without the word, fans knew the brand by the design.

While this decision might seem logical, "whether a trade dress can be confused with the word mark [distinctive text] of another company is without precedent," says Mark Evans, partner with Smart & Biggar/Fetherstonhaugh. "Typically you look at whether a word mark can be confused with another word mark and whether a trade dress can be confused with another trade dress."

Whether Canadian courts face such cases in the future seems to depend upon the confluence of an equally unique set of circumstances. "The court was very careful to indicate that the decision was tied to the particular facts in that case," Evans says.

Although it's unusual, trademarks can be owned by different entities in different countries. Gray notes that during the Second World War, German trademarks were seized in the United States. "After the war, there was confusion over who had rights to the trademarks," he says.

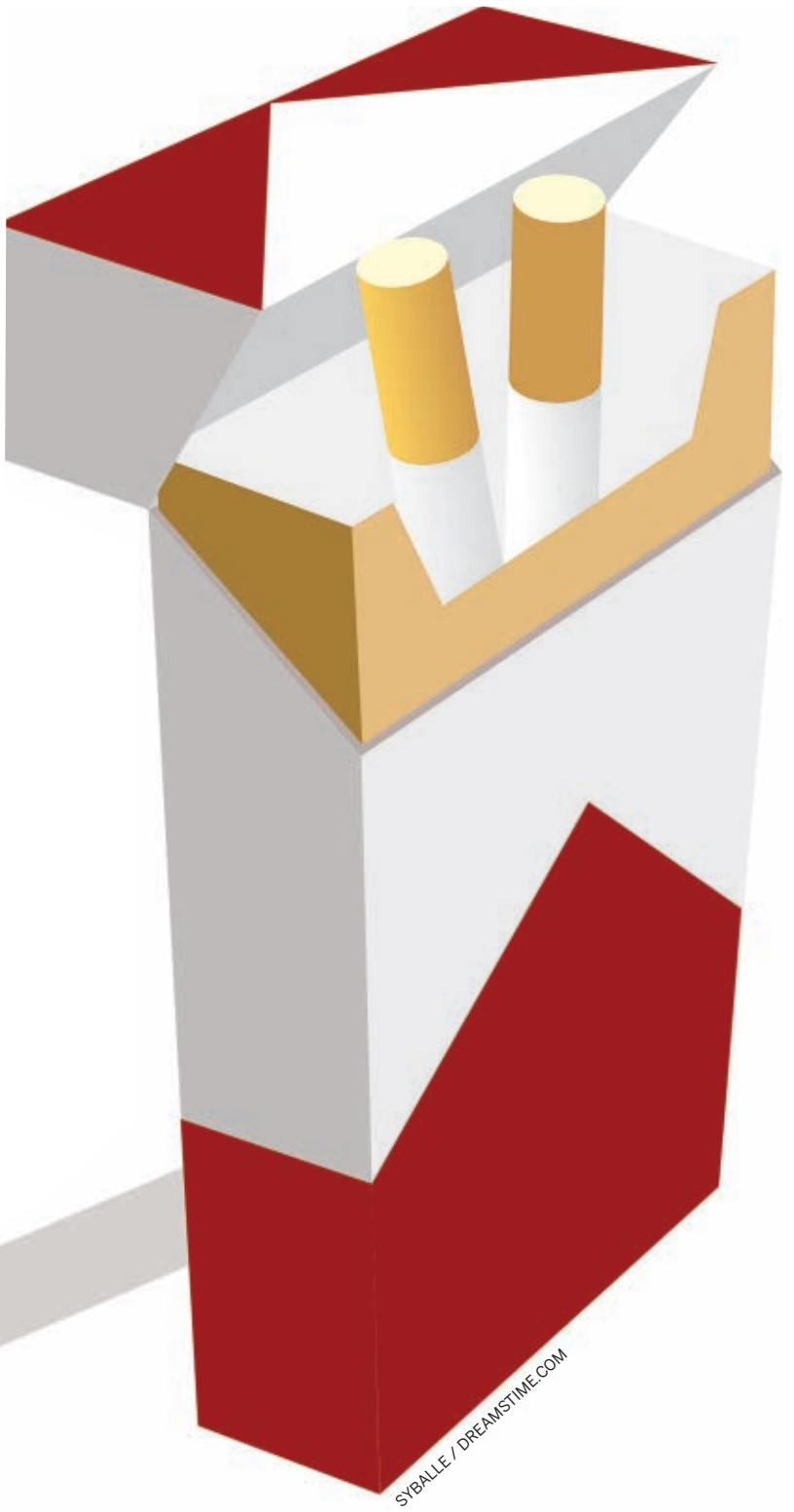
To an extent, Evans likened past cases to *Marlboro*. In *Ciba-Geigy Canada Ltd. v. Apotex Inc.* [1992] 3 S.C.R. 120, the court found one pharmaceutical company gave its products an appearance similar to those of a competitor.

Evans says it wasn't a matter of proving that doctors or pharmacists are confused. "It's sufficient if the patient was confused," he explains. "If the patient received a pharmaceutical product that had the same overall colour, shape and size as the brand name, and if that appearance serves as an indicator of source, then it would be possible to establish passing off."

In *Kirkbi AG v. Ritvik Holdings Inc.* [2005] 3 S.C.R. 302, a manufacturer created toy blocks that fit with Lego blocks. Even though people recognize that pattern of raised studs on a Lego block, the Supreme Court of Canada noted those studs perform a function. "As a matter of public interest, you cannot monopolize a utilitarian feature," Evans says.

In Canada, legislation is in the works to expand what Mark Davis calls an "antiquated" definition of a trademark. The new definition would include other indicia such as logos, sounds, holograms and so forth. "The MGM lion's roar was registered as a sound mark in the Canadian intellectual property office," says the

Confuse, Page 15



Focus INTELLECTUAL PROPERTY

The perils of third-party web storage

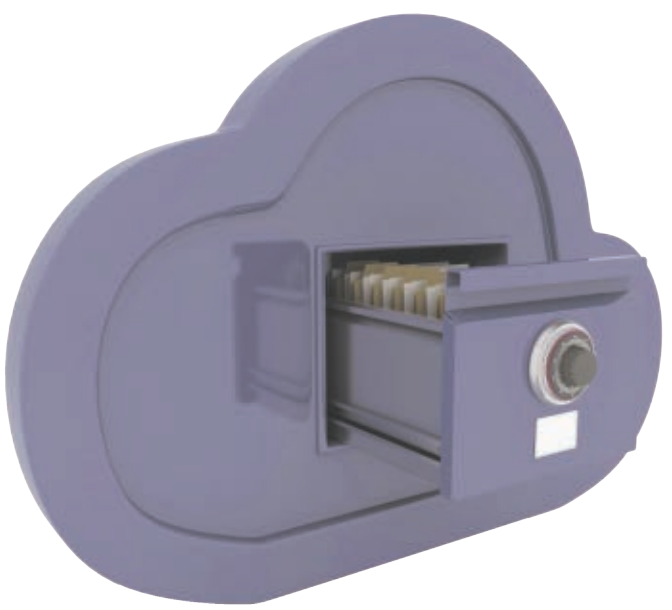
Jonathan Mesiano-Crookston

Edward Snowden blew the lid off America's spying activities around the world when he released top-secret information about surveillance programs operated by the National Security Agency, America's foreign signals intelligence gathering service.

Snowden, who worked for American intelligence for many years, spent the past year and a half working for two NSA contractors as an infrastructure analyst, which likely meant his job was figuring out how to break into computer systems and communications traffic around the globe. His high-level security clearance allowed him access to extremely sensitive information that described how the NSA collected and analysed Internet data flowing around the world.

In June, Snowden left his job, ostensibly to get treatment for a medical condition, and flew to Hong Kong where he started releasing the information he had collected to *The Guardian* in the U.K. and *The Washington Post* in the U.S.

And what a leak it was! The information he released included internal NSA training slides showing that the NSA had set up systems that collected and analyzed vast quantities of Internet traffic to determine the connections and patterns in peoples' communications. Other slides suggested that the NSA had the ability to collect information "directly" from the servers of such U.S.-based cloud computing providers as Google, Yahoo, and Microsoft. Exactly how this was done was not revealed, and the meaning of "directly" remains unclear.



KJPARGETER / DREAMSTIME.COM

While the revelation that all Internet communications are being tracked is not new (in 2006 a whistleblower alleged that AT&T's Internet backbone was being analyzed in bulk by the NSA), the recent release of Snowden's information has substantiated those worries. According to other releases of information, while the NSA typically portrays its role as being security-related (i.e., involving terrorism), it has been shown that the NSA is not beyond collecting the industrial and economic information of foreign countries.

Most people will not be the subject of an NSA order or warrant, but the release of Snowden's information serves as an excellent reminder for users of cloud computing services to be aware of the dangers of using public networks like the Internet, and when one provides data to third parties, to review internal and external security practices to ensure adequate data protection.

There is no such thing as perfect protection, but some valuable tips can ensure that you've done what you can to ensure your data is safe.

> "There is no such thing as perfect protection, but some valuable tips can ensure that you've done what you can to ensure your data is safe.
>
> **Jonathan Mesiano-Crookston**
> Goldman Hine

First, anyone using the Internet for secure purposes ought to assess if the data should be stored or sent to a third-party computer in the first place. Cloud services are run by third parties, and the data sent to them is only as secure as the practices of that third party. A few years ago, users of the file-storing service Dropbox were dismayed to learn that, over a period of several hours, the service allowed access to users' files without passwords because of a software glitch.

Secondly, always assess if the data is suitably protected by the third-party provider. Ask yourself the following questions: Do you know and trust the company well enough to trust your data with it? What are its policies on access to the data? Does it use recognized and standard encryption schemes? Does it have access to the encryption key to unlock your data, or does its service encrypt the information at your computer so the third party is unable to access the data?

As Snowden himself showed, the weakest link in a security regime is often the people. What are the service's practices with respect to physical access to your data? What countries does the company store your data in, and do those countries have legal structures that will adequately protect the security and privacy of your data?

Third, use secure communications to talk to the service. It doesn't make much sense to worry about 256-bit encryption schemes and strong passphrases if you send the information to the service in clear text.

Finally, how well do *you* use the service? Do you follow the service's recommended practices? Is your password strong enough (i.e. lengthy, and containing letters, numbers, and symbols) to withstand an attack, or can it be easily guessed? Also, are you securing the data on your end? If not, your own data store is the weak link in the chain.

The Snowden leak has been described as one of the worst security breaches in modern history. In the end, it may not have revealed anything new, as it was known that the NSA had been analyzing Internet traffic for years (and before that, telephone traffic). However, the Snowden affair serves as a poignant reminder to review your data-protection policies and practices, because Internet transmissions are not, and have never been, inherently secure. As we are occasionally reminded, sending unencrypted communications over the Internet is like sending a postcard: anybody in the path of the data can, if they want, read every word.

Jonathan Mesiano-Crookston is a patent and trademark agent and lawyer specializing in dispute resolution, franchising, technology, and intellectual property with Goldman Hine in Toronto.

Confuse: Courts view through eyes of consumer

Continued from page 14

Heenan Blaikie partner.

Davis perceives a constant in Supreme Court decisions. "What the courts look for is whether consumers are going to be confused," he says. The court doesn't "care how confusion is being created, but if it is being created (the court will) try to remedy that."

To protect intellectual property, an ounce of prevention seems to be the best cure. "You can register trade dress as a trademark with the Canadian trademarks office as a so-called 'distinguishing guise' so long as it isn't functional," Evans notes. "It can also be registered as an industrial design."

A few more ounces would come in handy. A company's advertising messages to the public "should emphasize that the appearance of the product is effectively a brand, an indicator of source," Evans adds. Hypothetically, should somebody decide to start a parcel delivery company and paint its trucks brown, UPS would very likely have an advantage in court.

Trade dress registration isn't enough to protect a brand. "Monitor the market and take action when a competitor steps over the line," Davis advises.

Meanwhile, companies need to carefully review their trademark portfolios. "If there's value there, the time and expense of registration is a relatively cheap insurance policy" against infringement, Davis says.