Canadian Journal of Law and Technology

Volume 12 | Number 2 Article 3

6-1-2014

With Great Power Comes Little Responsibility: The Role of Online Payment Service Providers with Regards to Websites Selling Counterfeit Goods

J. Bruce Richardson

With Great Power Comes Little Responsibility: The Role of Online Payment Service Providers with regards to Websites Selling Counterfeit Goods*

*J Bruce Richardson***

INTRODUCTION

Electronic Commerce, or e-commerce, as the name suggests, is essentially the electronic version of commerce. Retail e-commerce in Canada totalled $15.3 billion in 2010, which was double the 2005 level.[1] This increase in online business activity would suggest a corresponding increase in online illegitimate business activity. The sale of counterfeit goods in places like flea markets and malls has now moved into the online world with flashy websites and easy-to-access payment services. If websites devoted to the sale of counterfeit goods are becoming more prevalent with the ease of e-commerce, would this correspond to trademark owners' ease in enforcing their rights online?

One aspect in which an e-commerce website is different than a bricks-and-mortar retail store is that the website must be able to accept electronic payments; cash-only transactions are not possible.[2] These electronic payments are conducted through online payment networks administered by companies such as Visa and MasterCard. Being the backbone of e-commerce, it is vital that Merchants have access to these online payment networks. If Visa or MasterCard were to cut off their services to a certain website, the ability of that website to engage in e-commerce would, effectively, be removed.

This would seem to give much power to such companies, but what about their obligations? Should there be a duty on such companies that provide electronic payment services to cease or withhold those services to websites that are dedicated to

---

* An earlier draft of this article was the major paper to complete my LL.M. in Law and Technology. I am indebted to Prof. Teresa Scassa, Courtney Doagoo, and Glenn Walsh for their thoughtful and invaluable comments on earlier drafts.

** M.Sc. (Laval, 1996), LL.B. (UOttawa, 1999), LL.M. (UOttawa, 2014). Currently working as a policy analyst for the Copyright and Trademark Policy Directorate at Industry Canada. While I work for the Government of Canada, this is entirely my own initiative and what I state here does not necessarily reflect the views of my employer, my office, or my position.

1 Report of the Standing Committee on Industry, Science and Technology, *E-Commerce in Canada: Pursuing the Promise*, 41st Parl 1st Sess May 2012, at 5, online: <http://www.parl.gc.ca/>.

2 One possibility for online payments without the use of credit or debit cards is through BitCoin, which is a type of digital currency. However, this is not currently a widely-available option for e-commerce Consumers in the way that Visa, MasterCard, or PayPal are, so this article will focus on the more conventional options.

the sale of counterfeit goods? If so, what options are available to policy makers to create this duty? Is there a preferred option? And what about the Merchants; if they are accused of counterfeiting online, what rights do they have?

This article will explain the current avenues for intellectual property rights holders to make use of existing anti-counterfeiting policies made available by financial companies dealing in electronic payments, and argue that current policies, while helpful, are not sufficient. The article will conclude by demonstrating that policy makers have options to intervene and regulate the use of online payment services, either directly through legislation or indirectly through facilitating "best practices."

I. E-COMMERCE TRANSACTION PROCESSING

In order to sell goods or services through a website, the website owner must set up a system to gain access to a network that processes electronic payments. As we shall see, someone wishing to create their own e-commerce website can obtain access to these networks only through an intermediary. In this section, we outline the players involved in a typical banking transaction, and the role these intermediaries play.

(a) Banking Players

A typical online banking transaction to purchase goods involves several players: Consumers, Issuers, Merchants, Acquirers, and Payment Network Associations.

(i) Customer and Issuer

The *Customer* is the person holding the payment card (such as a credit card). The bank that issues the credit card to the Customer is called the *Issuer*. The contract between the Issuer and the Customer will contain terms such as the interest rate of the card, the limit the Customer can spend, and penalties for late payments or for spending above the limit. The Issuer will guarantee the debt on a credit card while the Customer will promise to pay back any debt accrued on the card.

(ii) Merchant and Acquirer

On the other side of the transaction is the *Merchant*; the entity selling the goods. In order to provide the ability for the Customer to purchase goods and services, the Merchant needs an entity able to process the online card payments. This entity is the acquiring bank, called the *Acquirer*. The Acquirer enters into a contract with the Merchant and offers it a Merchant Account,[3] which is essentially a line of credit. The Acquirer of the Merchant interacts with the Issuer of the Customer, and deals with any exchange rates, interchange fees, etc.

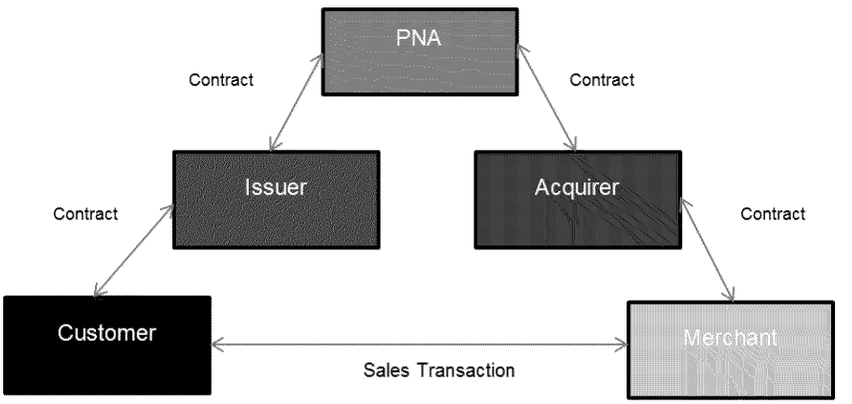
---

3 "Merchant Accounts", online: Merchant Warehouse <http://merchantwarehouse.com/glossary/merchant-accounts>.

(iii) Payment Network Associations

In the middle of these players is the *Payment Network Association*[4] (PNA). These companies provide the electronic system required to enable transactions to occur. They will enter into separate contracts with the Issuer and with the Acquirer. A PNA is responsible for, among other things, securing the network for payment processing, developing new marketplace opportunities, while promoting its global brand. The more secure Customers feel about using the credit card, the more Merchants will want to offer that card as a payment option.

A graphical display of these relationships is found below:



(b) Typical Online Transaction

A typical online transaction with a credit card will go through seven stages:

1. Purchase: The cardholding Customer selects goods and/or services for purchase, and inputs the credit card information on the website.

2. Merchant Submission: At the time of purchase, the Merchant's website submits the Customer's purchase details, including the card information and payment amount, to its Acquirer for processing and authorization.

3. Analysis: The Acquirer takes the information submitted by the Merchant and sends the information along to the PNA. The PNA receives the request and analyses the transaction for potential fraud, determines the type of transaction, then identifies the Issuer. Once this information is determined, the PNA forwards the authorization request to that Issuer.

---

4 Some literature will use the term "Financial Transaction Provider", but that would include all financial institutions (Issuers and Acquirers). For the purposes of this article, the companies in charge of administering the payment networks will be considered separate from the financial companies that deal with Merchants or issue credit cards.

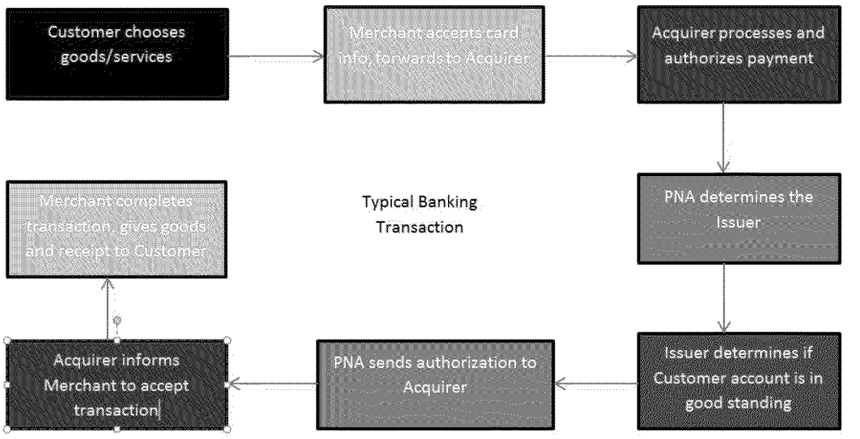
4. Determination of Credit: The Issuer then identifies the Customer's account, ensures that the account is in good standing, and verifies that the value of the transaction fits within the cardholder's limit.

5. Approval: The Issuer approves the purchase and instructs the PNA to send its authorization of purchase approval to the Acquirer.

6. Notification to Merchant: The Acquirer will receive the authorization for the sale from the PNA and forward this purchase approval message to the Merchant to complete the transaction. Once the Issuer has approved the transaction, payment is guaranteed for the Merchant.

7. Sale: The Merchant receives the authorization response for the purchase and guarantee of payment, and the Customer is notified that the purchase has been accepted, usually through a separate webpage detailing the transaction, followed by a printed invoice.

A graphical display of these steps is found below:



All of these steps transpire in a matter of seconds. It is interesting to note that in a typical transaction, the PNA is never directly in touch with either the Customer or the Merchant. Direct dealings occur only with the Issuer or the Acquirer.

(c) Payment Network Associations

As mentioned above, PNAs administer the networks over which these online financial transactions take place. Two of the more popular PNAs are Visa and MasterCard.[5]

---

5 Another PNA that administers a payment network is Interac. Based in Canada, Interac administers debit card transactions. This article will focus on credit card networks that, as we shall see, have developed anti-counterfeiting policies.

(i) Visa

Visa does not identify itself as a "credit card" company. Rather, it claims to be a "global payments technology company"[6] that allows Customers to use available funds electronically to connect to Merchants without the use of hard cash or cheques. Visa handled a total of 85.5 billion transactions in 2013, which works out to more than 47,000 transactions *per second*, amounting to a total volume of $6.9 trillion.[7]

(ii) MasterCard

MasterCard also refers to itself as a "technology company" as opposed to a credit card company:

> What We Don't Do
>
> We don't issue cards, set interest rates or establish annual fees. Those decisions are made by card issuers, such as banks. We don't set merchant discount rates either. Acquirers do that. And, of course, we don't make money from interchange fees.[8]

There are currently 1.9 billion MasterCard credit cards, accounting for $3.6 trillion among over 210 countries.[9] MasterCard processes over 65,000 transactions every minute.[10]

(d) Issuers

In Canada, there are many financial institutions that issue credit cards to Customers. Visa cards may be obtained from banks such as Royal Bank of Canada (RBC), Canadian Imperial Bank of Commerce (CIBC), TD Canada Trust, and Scotiabank.[11] MasterCard credit cards may be issued by the Bank of Montreal, MBNA (a subsidiary of TD Canada Trust), RBC through a joint venture with WestJet, and President's Choice Financial.[12]

---

6 "About Visa", online: Visa USA <http://usa.visa.com/about-visa/index.jsp >.

7 "Global Presence", online: Visa USA <http://usa.visa.com/about-visa/our-business/global-presence.jsp>.

8 "About Us", online: MasterCard Worldwide USA <http://www.mastercard.com/corporate/ourcompany/about-us.html>.

9 MasterCardWorldwide, "MasterCard — By the Numbers" (21 March 2013), online: YouTube <http://www.youtube.com/watch?v=zgq4FvrIOe0>. Figures are from 2012.

10 *Ibid.*

11 For a definitive list, see "Personal Card Option — Get a Card" online: Visa Canada <http://www.visa.ca/en/personal/getcard.jsp>.

12 Several types of MasterCards may be found here: "Find A Credit Card" online: <http://www.mastercard.ca/find-a-credit-card.html>.

(e) Acquirers

There are many examples of Acquirers, particularly those that specialize in e-commerce. Wikipedia lists sixty-five different online payment service providers.[13] Some websites are devoted to helping Merchants pick a payment service provider that is right for them.[14] This article will consider three of the more popular Acquirers.

(i) PayPal

Acquired by eBay in 2002, PayPal was the result of a merger of two online financial payment companies, Confinity and X.com.[15] According to its website, PayPal managed 143 million accounts in 193 markets and twenty-six currencies around the world, processing more than nine million payments a day in 2011.[16]

In a typical transaction, PayPal will act as an Acquirer and provide information sent by the Merchant to the Issuer of the Customer.[17]

(ii) Moneris

Moneris is another Acquirer available to Canadian Merchants. Moneris started as a joint investment between Royal Bank Financial Group and Bank of Montreal Financial Group in 2000.[18] The company processes more than three billion credit and debit card transactions a year for over 350,000 Merchant locations across North America.[19]

---

13 "List of online payment service providers", online: Wikipedia <http://en.wikipedia.org/wiki/List_of_online_payment_service_providers>.

14 For some examples, see "Selecting a Payment Service Provider", online: PayPoint.net <http://www.paypoint.net/support/online-payment-guides/select-payment-service-provider/>, "18 Online Payment Services and System", online: Awwwards <http://www.awwwards.com/18-online-payment-services-and-systems.html>, and Susan Ward, "Online Payment Options for Your Online Business", online: About.com <http://sbinfocanada.about.com/od/onlinebusiness/a/onlinepayment.htm>.

15 "Elon Musk Biography", online: Encycolpedia of World Biography <http://www.notablebiographies.com/news/Li-Ou/Musk-Elon.html>.

16 "About PayPal", online: PayPal USA <https://www.paypal-media.com/about>.

17 The information is not limited to the Customer's credit card. The Customer may list several credit cards as well as debit bank accounts in the PayPal account. PayPal will make inquiries about each bank account registered (and with each Issuer) with the Customer's profile, starting with the Primary bank account. If the Issuer returns information saying that the funds are not available for that account, PayPal will make an inquiry about the next account in the Customer's profile, and so on down the list until one of the accounts has the requisite funds. If none of the Customer's bank accounts have the funds, PayPal will direct the Merchant not to accept the Customer's payment.

18 "Corporate Profile", online: Moneris Solutions <http://www.moneris.com/Home/About-Moneris/Corporate-Profile.aspx>.

19 *Ibid.*

(iii) Amazon Payments

Amazon Payments is a subsidiary of Amazon.com that, similar to PayPal, can provide a means to process online payments. Much like eBay Customers who have instant access to PayPal, Amazon.com users can access Amazon Payments to make their purchases. Also like PayPal, Customers can use Amazon Payments to access their Visa or MasterCard accounts to purchase goods and services online. Amazon Payments is not available to Merchants in Canada.[20]

Counterfeit goods are frequently sold online using these payment mechanisms. Before considering whether any remedy can be sought through any of the players in a typical online payment transaction, a trademark owner will first have to establish that their trademark rights have been infringed. Infringement in the online context is considered in the next section.

II. TRADEMARK PRINCIPLES ON THE INTERNET

There is a general consensus internationally that trademark protection under domestic law should extend to the Internet, and that its scope should be neither less nor more extensive than the protection granted in the physical world.[21] The Canadian government has agreed with this position, stating that the laws in the virtual world should be consistent with those in the real world as much as possible, and that one of the first principles of the organization of the Internet is that measures need to be "efficient, cost effective and administratively non-burdensome".[22]

When e-commerce became popular, many businesses began establishing a web presence.[23] Obviously, disputes arising between companies in the real world would not cease once companies began to move into the virtual sphere, but these new technological advances required new thinking to determine how established trademark principles would apply.[24] Trademark principles of infringement, use,

---

20 "Checkout by Amazon FAQ", online: Amazon Payments <https://payments.amazon.com/help/Checkout-by-Amazon/Checkout-by-Amazon-FAQ>. Although not available for Canadian Merchants, Amazon Payments may be used by Canadian Customers through their amazon.ca accounts.

21 WIPO, *Intellectual Property on the Internet: A Survey of Issues*, WIPO Doc WIPO/INT/02 (2002) at 64-65, online: WIPO <http://www.wipo.int/copyright/en/ecommerce/ip_survey/>.

22 WIPO, Standing Committee on Trademarks, Industrial Designs and Geographical Indications (SCT), *Second Special Session on the Report of the Second WIPO Internet Domain Name Process: Report*, WIPO Doc SCT/S2/08 (2002), 2d Spec Sess at para 70, online: WIPO <http://www.wipo.int/edocs/mdocs/sct/en/sct_s2/sct_s2_8.pdf>. This intervention was mostly in the context of domain name administration.

23 The number of registered dot-ca domain names rose from 140,000 in 2000 to one million in 2010, to over two million today; "History": online <http://www.cira.ca/about-cira/history/>. For an interesting article on the first "wild days" of domain name registration, see Joshua Quittner, "Right now, there are no rules to keep you from owning a bitchin' corporate name as your own Internet address", *Wired* (1993), online: Wired <http://www.wired.com/wired/archive/2.10/mcdonalds_pr.html>.

24 Brian G Gilpin, "Trademarks in Cyberspace: Fulfilling the 'Use' Requirement through the Internet" (1996) 78:12 J Pat & Trademark Off Soc'y 830; Dennis M Kennedy,

and enforcement all had to be re-evaluated in the context of e-commerce.[25] Trademark law, which is territorial in scope, had to be modified for the Internet, which is global in scope. In some cases, existing trademark principles were simply adjusted to apply to the online context (e.g. "initial interest confusion"),[26] while in other cases, whole new laws and principles were created.[27]

(a) Counterfeiting

The *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPs) offers a definition of "counterfeit trademark goods" in the context of border measures:

> "counterfeit trademark goods" shall mean any goods, including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such goods, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the owner of the trademark in question under the law of the country of importation.[28]

Although this definition was meant to apply to border measures, its scope has been incorporated into civil causes of action. In fact, in the trademark section of the

---

"Key Legal Concerns in E-Commerce: The Law Comes to the New Frontier" (2001) 18:1 TM Cooley L Rev 17; Xuan-Thao N Nguyen, "Shifting the Paradigm in E-Commerce: Move over Inherently Distinctive Trademarks — The E-Brand, I-Brand and Generic Domain Names Ascending to Power?" (2001) 50 Am U L Rev 937.

25 Despite the words of Electronic Frontier Foundation co-founder John Perry Barlow, who claimed, "Your legal concepts of property, expression, identity, movement, and context do not apply to us. They are all based on matter, and there is no matter here." John Perry Barlow, "A Declaration of the Independence of Cyberspace" (8 February 1996), reprinted in Daniel Castro, "A Declaration of the Interdependence of Cyberspace", *Computer World* (8 February 2013), online: Computer World <http://www.computerworld.com/s/article/9236603/A_Declaration_of_the_Interdependence_of_Cyberspace>.

26 Although the initial interest confusion doctrine has gained some recent notoriety through its application online, the doctrine has been in use for a long time. See Ilanah Simon Fhima, "Initial interest confusion" (2013) 8:4 J Intell Prop L & Prac 311; Helen Norton & Danielle Keats Citron, "Confusion in Cyberspace: Defending and Recalibrating the Initial Interest Confusion Doctrine" (2004) 117:7 Harv L Rev 2387 at 2392.

27 The Uniform Domain-Name Dispute Resolution Policy (UDRP) is an international administrative procedure to allow trademark owners to have domain names containing their trademarks be transferred back to them, or removed from the domain name space altogether. The *Anticybersquatting Consumer Protection Act* (*Lanham Act*, 15 USC §1125(d) [ACPA]) was enacted in the U.S. giving new tools to trademark owners to fight cybersquatting. For details on their creation, see Jason M Osborn, "Effective and Complementary Solutions to Domain name Disputes: ICANN's Uniform Domain Name Dispute Resolution Policy and the *Federal Anticybersquatting Consumer Protection Act of 1999*" (2000) 76 Notre Dame L Rev 209.

28 *Agreement Establishing the World Trade Organization, Annex 1C: Agreement on Trade-Related Aspects of Intellectual Property Rights*, 15 April 1994, 1869 UNTS 299, art 51 fn 14(a) [TRIPs].

TRIPs Agreement, the rights conferred upon the owner of a registered trademark are based on the finding of a likelihood of consumer confusion, except in the case of "the use of an identical sign for identical goods or services"[29] where Member States are to create a presumption of confusion. This particular activity must have been considered particularly egregious.

Although there is no definition of the term "counterfeit" in the Canadian *Trade-marks Act* (TMA),[30] the term is often used in Canadian judgments to denote the situation where an identical trademark is used on identical goods found in the registration.[31] A classic counterfeiting case requires the plaintiff to show that the defendant used an identical trademark on identical goods.

(b) Infringement

Internet use of trademarks can be challenged in two ways. For unregistered trademarks, the tort of passing off is available. For registered trademarks, infringement provisions in the TMA can be invoked.[32] Section 19 defines the exclusive right granted to the owner of a registered trademark:

> . . . the registration of a trade-mark in respect of any wares or services, unless shown to be invalid, gives to the owner of the trade-mark the exclusive right to the use throughout Canada of the trade-mark in respect of those wares or services.[33]

Any unauthorized use of a registered trademark, anywhere in Canada, would be a violation of this section. Case law suggests that section 19 applies in situations where an identical mark was used in association with identical goods or services (thus meeting Canada's obligation under article 16.1 of TRIPs).[34] Such cases would be classic counterfeiting situations. For our purposes, the act of "counterfeit-

---

29 *Ibid* at art 16.1.

30 RSC 1985, c T-13 [TMA].

31 *Moroccanoil Israel Ltd. v. Lipton*, 2013 FC 667, 2013 CarswellNat 2114, 2013 CarswellNat 2826 (F.C.) at para 7 (available on CanLII); *Harley-Davidson Motor Co. Group LLC v. Manoukian*, 2013 CarswellNat 449, 2013 FC 193, 112 C.P.R. (4th) 404 (F.C.), at para 1. Note that the term "counterfeiting" is found within s. 53.3(b) of the TMA, which was created when Canada amended its IP laws to adhere to TRIPs. The detention proceedings have been used only a handful of times, so no case law has tackled the use of this term and its corresponding definition.

32 Note that section 7 of the *Trade-marks Act* essentially codifies the common law tort of passing off (*Kirkbi AG v. Ritvik Holdings Inc. / Gestions Ritvik Inc.*, 2005 SCC 65, [2005] 3 S.C.R. 302, 2005 CarswellNat 3632, 2005 CarswellNat 3631 (S.C.C.)), and has been used by owners of registered trademarks to seek damages when the infringement provisions are not helpful. For the purposes of this article, I will be focussing on the infringement provisions in the TMA.

33 *Ibid* at s. 19.

34 *Canadian Council of Blue Cross Plans v. Blue Cross Beauty Products Inc.*, 1971 CarswellNat 250F, 1971 CarswellNat 250, [1971] F.C. 543, 3 C.P.R. (2d) 223 (Fed. T.D.); *Cie générale des établissements Michelin — Michelin & Cie v. CAW-Canada*, 1996 CarswellNat 2711, 71 C.P.R. (3d) 348, [1997] 2 F.C. 306, 1996 CarswellNat 2297 (Fed. T.D.) at 358.

ing" will be limited to cases where section 19 would apply: identical trademarks used on identical goods.[35]

(c) Use

Trademark use by a defendant is fundamental to a finding of trademark infringement.[36] Thus, in order for section 19 to apply, a plaintiff would have to establish that the trademark in question was "used" in association with the sale of goods.[37] This is defined under the *Trade-marks Act*:

> A trade-mark is deemed to be used in association with wares if, at the time of the transfer of the property in or possession of the wares, in the normal course of trade, it is marked on the wares themselves or on the packages in which they are distributed or it is in any other manner so associated with the wares that notice of the association is then given to the person to whom the property or possession is transferred.[38]

There are several elements that must be present in order to find that a trademark was "used" in association with goods: 1) "normal course of trade"; 2) "in association with wares"; and 3) "at the time of the transfer of the property in or possession of the wares".

(i) "Normal course of trade"

Although there is much case law on what activities fall under the element of "normal course of trade",[39] courts have held that it is not up to them to establish standards or definitions here; rather, use in the "normal course of trade" will be

---

35 Although infringement actions under sections 20 or 22 are important to trademark owners, those sections generally go beyond the narrow case of an identical trademark used on an identical good.

36 For a more detailed discussion of trademark use in Canada, see Daniel R. Bereskin, QC, "Chapter 4: Trade-mark Use" in Gordon F. Henderson, ed., *Trade-marks Law of Canada* (Toronto: Carswell, 1993) at 97; Sheldon Burshtein "The Basics of Trademark Use in Canada: The Who, What, Where, When, Why and How" (1997) 11 IPJ 229 (Part I) and (1998) 12 IPJ 75 (Part 2), and; David Vaver, *Intellectual Property Law: Copyright, Patents, Trade-marks* (Toronto: Irwin Law, 2011) at 471ff. For discussion on trademark use with respect to s. 19, see Teresa Scassa, *Canadian Trademark Law* (Markham, ON: LexisNexis Canada, 2010) at 354. For a take on how the use requirement has been misapplied, see Uli Widmaier, "Use, Liability, and the Structure of Trademark Law" (2004) 33 Hofstra L R 603; and Stacey L. Dogan and Mark A. Lemley, "Grounding Trademark Law Through Trademark Use" (2007) 92 Iowa L Rev 1669.

37 Section 2 of the TMA defines "trade-mark" as "a mark that is *used* by a person for the purpose of distinguishing . . ." [emphasis added].

38 TMA, s*upra* note 30 s 4(1).

39 For example, courts have looked at the supply chain to determine if particular activities fall out of that chain; *Manhattan Industries Inc. v. Princeton Manufacturing Ltd.*, 1971 CarswellNat 513, 4 C.P.R. (2d) 6 (Fed. T.D.) [*Manhattan Industries*], or if a statutory regime requires government approval, sales outside that approval may not meet this element; *Molson Cos. v. Halter*, 1976 CarswellNat 487, 28 C.P.R. (2d) 158 (Fed. T.D.).

considered on a case-by-case basis.[40] At a minimum, there has to be a commercial use.[41] Second-hand sales would not count.[42] A website giving away goods for free, or dealing in parallel import goods, probably would not fulfil this element.[43]

(ii) "In association with the goods"

The trademark also needs to be used in association with the goods. The obvious way is for the trademark to be branded onto the good itself, or attached to the good through packaging or a tag. In cases where a trademark cannot be easily "attached" to the good (e.g. downloaded software), it is sufficient for the trademark to appear elsewhere so long as there is notice to the transferee before and after the sale of the goods.[44] In the online environment, what would be considered "sufficient notice"? Arguably, if the website has a picture of the good showing the trademark either on the packaging or marked on the goods themselves, then it would be sufficient notice before the sale. If the Customer is brought to another web page where a

---

40 *Institut national des appellations d'origine des vins & eaux-de-vie v. Canada (Registrar of Trade Marks)* (1983), 71 C.P.R. (2d) 1, 1983 CarswellNat 658 (Fed. T.D.), at 5 [C.P.R.].

41 *Cast Iron Soil Pipe Institute v. Concourse International Trading Inc.*, 1988 CarswellNat 1522, 19 C.P.R. (3d) 393 (T.M. Opp. Bd.); *Osler, Hoskin & Harcourt v. Rogers Foods Ltd.* (1994), 1994 CarswellNat 3027, 53 C.P.R. (3d) 570 (T.M. Opp. Bd.), at 571 [C.P.R.]; *Renaud Cointreau & Cie v. Cordon Bleu International Ltd.*, 1993 CarswellNat 2586, 52 C.P.R. (3d) 284 (T.M. Opp. Bd.); affirmed (2000), 188 F.T.R. 29, 2000 CarswellNat 3354, 2000 CarswellNat 2137, 10 C.P.R. (4th) 367 (Fed. T.D.).

42 The doctrine of first use states that a trademark owner loses its exclusive right after the first sale of a good bearing the owner's trademark, so long as that first sale was done in the ordinary course of business. Any re-sale of that good is not "use" under the TMA. See *Coca-Cola Ltd. v. Pardhan*, 1997 CarswellNat 4141, 1997 CarswellNat 2212 (Fed. T.D.), at para 18, ; affirmed 1999 CarswellNat 598, 1999 CarswellNat 4765 (Fed. C.A.); leave to appeal refused 2000 CarswellNat 721, 2000 CarswellNat 722 (S.C.C.); *Smith & Nephew Inc. v. Glen Oak Inc.*, 1996 CarswellNat 734, [1996] 3 F.C. 565, 68 C.P.R. (3d) 153, 1996 CarswellNat 2588 (Fed. C.A.); leave to appeal refused 1997 CarswellNat 3251 (S.C.C.) [*Smith & Nephew*]. This doctrine has limits in the context of trademark law, where goods are repackaged or modified then sold with the trademark affixed. See David W Barnes, "Free-Riders and Trademark Law's First Sale Rule" (2011) 27:3 Santa Clara Computer & High Tech LJ 457.

43 Goods that are legally obtained abroad and imported into Canada are often called "parallel imports" or "grey goods". These are generally not considered to be counterfeit since the trademarks owner is said to have exhausted its rights upon the first sale. See *Smith & Nephew*, *supra* note 42. In Canada, case law has held that goods that are substantially different enough to cause confusion would not be considered parallel imports; *H.J. Heinz Co. of Canada v. Edan Food Sales Inc.*, 1991 CarswellNat 179, 35 C.P.R. (3d) 213 (Fed. T.D.).

44 *Mumm & Cie v. Andres Wines Ltd.*, 1984 CarswellNat 599, 3 C.P.R. (3d) 199, 3 C.I.P.R. 277 (Fed. T.D.), at 201 [C.P.R.]; *BMB Compuscience Canada Ltd. v. Bramalea Ltd.*, 1988 CarswellNat 730, 1988 CarswellNat 589, 22 C.P.R. (3d) 561 (Fed. T.D.) at 570 [C.P.R.]; *Dominion Automotive Group Inc. v. Firebolt Engine Installation Centres Inc.*, 1998 CarswellNat 3020, 86 C.P.R. (3d) 403 (T.M. Opp. Bd.) at 411 [C.P.R.].

receipt can be printed, is that sufficient notice after the sale? There is precedent that if a trademark is found in the body of an invoice, then there is use in association with the good.[45] This may be enough to apply in the online world.

(iii) "At the time of the transfer of the property in or possession of the wares"

There needs to be actual possession, or at least the eventual possession, of the goods.[46] The website would have to be more than simply advertising the goods; there has to be the ability for a Customer to attain the goods. A website merely advertising computers for sale, while not offering them for sale, is a "passive" website and therefore does not meet the "use" requirement.[47] Arguably, if the website actually allowed Customers to buy the computers through the website, this element would have been satisfied.

(d) Enforcement

Once a registered trademark owner is successful in proving all these elements, and shows that there has been use of its trademark on a website, there still remains the enforcement of the owner's rights. This would involve sending a cease-and-desist letter, or seeking an injunction order from the courts. This can prove to be a daunting task in an online context. Finding the owner of a website is not necessarily as easy as finding the owner of a retail store. Websites are incredibly easy to set up, and domain name registration is quick, cheap, and simple, so the website owner could, literally, reside anywhere in the world. It is also possible to obtain a website and domain name anonymously, which makes it even more difficult to find the website owner and send any letters.

The U.S. has been able to address this possibility by allowing trademark owners to sue not only a domain name owner, but the domain name itself.[48] Regardless of where the domain name owner resides, a trademark owner can go to court and have the domain name de-registered, or transferred over to the trademark holder. U.S. policy makers attempted to expand this right of action to include not only domain names containing trademarks, but to websites being used to sell counterfeit goods online.[49] Such laws work in the U.S. mainly because most of the Internet Registrars reside in the U.S., and therefore would be susceptible to any court orders given by a U.S. court. Website owners need to have their websites hosted some-

---

45 *Hortilux Schreder B.V. v. Iwasaki Electric Co.*, 2012 CarswellNat 5640, 2012 CarswellNat 4836, 2012 FCA 321 (F.C.A.); *3082833 Nova Scotia Co. v. Lang Michener LLP*, 2009 FC 928, 2009 CarswellNat 2886, 2009 CarswellNat 6626 (F.C.).

46 *Manhattan Industries*, *supra* note 39.

47 *Pro-C Ltd. v. Computer City Inc.*, 2001 CarswellOnt 3115, 14 C.P.R. (4th) 441 (Ont. C.A.); leave to appeal refused 2001 CarswellOnt 5075, 2001 CarswellOnt 5074 (S.C.C.). This particular case failed on the transfer of property element, since no transfer of ownership was found (at para 14). See also *Syntex Inc. v. Apotex Inc.*, 1984 CarswellNat 807, 1 C.P.R. (3d) 145, 1984 CarswellNat 653 (Fed. C.A.) at 151 [C.P.R.].

48 ACPA, *supra* note 27. A person can sue a domain name *in rem* when the person owning the domain name is unattainable after a reasonable search.

49 See *infra* note 115.

where, and that "somewhere" is usually found through U.S.-based companies.[50] Although Canadian trademark owners face similar problems, there is no fast and easy solution. Finding a website owner is one thing; getting a court order to enjoin that person from doing certain activities on that website is quite another.

Instead of a direct attempt to shut down a website as discussed above, there may be a more indirect way. One aspect that all these websites have in common is the ability to accept online payments for the counterfeit goods. In order to purchase the counterfeit goods, the Customer will have to use either a credit or debit card to transfer the money to the Merchant. In such cases, some Payment Network Associations and Acquirers have voluntarily created policies available to an IP rights holder.

III. ANTI-COUNTERFEITING POLICIES

What, if anything, can PNAs do to either stop individual transactions, or get an offending website taken down? Online payment services are the life-blood of any website dealing with e-commerce, including would-be counterfeiters hoping to sell such goods online. In theory, if there were no way of accepting online transactions, then the website would "die", in the sense that it could no longer offer goods for sale. An analogy would be confiscating all of the money tills at a flea market, thus preventing any of the Merchants there from making any transactions. Any goods, although visible to Consumers, could not be purchased.

(a) PNAs

(i) Visa

Visa voluntarily offers trademark owners some assistance. Upon receiving information and evidence directly from the trademark owner establishing that a Merchant is using Visa-brand payment services to sell counterfeit goods online, Visa will attempt to identify and notify the Merchant's acquiring bank (the Acquirer).[51] The Acquirer would be asked to investigate the allegation of counterfeiting. If the Merchant refuses to cease selling the goods at issue, or does not provide any evidence that the sale of the goods is lawful, the Acquirer is expected to terminate processing Visa payments for the Merchant.[52] If the Merchant provides such evidence (that the sale of the goods is lawful) in writing, the information will be provided to the trademark owner and direct that owner to address concerns directly with the Merchant or the Acquirer.[53] At Visa's discretion, a trademark owner may

---

50 GoDaddy, the largest Internet Registrar, provides web hosting services to over 12 million entities world-wide; "US-based domain registrar GoDaddy prepares to go public", *Venture Capital Post* (14 March 2014), online: Venture Capital Post <http://www.vcpost.com/articles/22548/20140314/us-based-domain-registrar-godaddy-prepares-to-go-public.htm>.

51 "Intellectual Property Rights", online: Visa USA <http://usa.visa.com/about-visa/our-business/intellectual-property-rights.jsp>.

52 *Ibid.*

53 *Ibid.*

be required to indemnify Visa against any claim by the Merchant or other affected parties relating to the investigation or any subsequent remedial action.[54]

Before addressing the Acquirer, Visa seeks:

> 1. a detailed description of each counterfeit good, including the name of the good, the model number (if applicable), and screenshots showing each counterfeit good appearing on the Merchant's website;
>
> 2. evidence that the trademark owner has already made enforcement efforts, such as cease and desist letters to the Merchant and any other enforcement-related documentation evidencing the trademark owner's own good faith attempts to enforce its rights;
>
> 3. evidence that the counterfeit goods can be purchased using a Visa payment card (for example, a screenshot showing the Visa logo being used on the Merchant website at check-out, or better yet, a screenshot of the invoice webpage after goods have been purchased).[55]

Although Visa gives direction to the Acquirer regarding investigations, the consequences of the Acquirer's failure to investigate are unclear. This is in contrast with MasterCard's policy, as we will see below.

(ii) MasterCard

MasterCard addresses intellectual property infringement in different ways depending on the person inquiring. When a law enforcement entity is involved in the investigation of online sales of counterfeit goods, and provides MasterCard with evidence of this illegal activity, MasterCard will identify the Acquirer that has the relationship with that Merchant alleged to be selling the counterfeit goods. If MasterCard determines that the Merchant is accepting MasterCard card payments through an existing Acquirer relationship, it will require that the Acquirer investigate the alleged illegal activity and, within two days, provide a written report back to MasterCard.[56]

Another possibility is that IP rights holders may notify MasterCard directly even if there is no law enforcement entity involved by sending an email to a special MasterCard email account set up for such inquiries.[57] The notification and request must include four pieces of information:

> 1. a description of the alleged infringement, including the URL of the website and compelling evidence substantiating the allegation, and the identity of the counterfeit products;
>
> 2. evidence that the counterfeits can be purchased using a MasterCard (e.g. a screenshot with the MasterCard logo);
>
> 3. a copy of the right holder's cease and desist letter to the Merchant; and

---

54 *Ibid.*

55 *Ibid.*

56 "MasterCard Anti-Piracy Policy", online: MasterCard <https://www.mastercard.com/us/wce/PDF/MasterCard_Anti-Piracy_Policy.pdf> at 1.

57 The special email is ipinquiries@mastercard.com, *ibid* at 2.

4. evidence of ownership of the trademark (e.g. a copy of the trademark registration).[58]

MasterCard will then attempt to identify the Acquirer that has the relationship with the Merchant. If MasterCard determines that the Merchant is, in fact, accepting MasterCard card payments through an existing Acquirer relationship, MasterCard will forward the trademark owner's request to the Acquirer, who must investigate the alleged activity and, within five business days, provide a written report back to MasterCard.[59]

If the Acquirer determines that the Merchant was engaged in the sale of counterfeit goods, the Acquirer must take the actions necessary to ensure that the Merchant has "ceased accepting MasterCard as payment"[60] for the counterfeit goods. If the Acquirer determines that the Merchant was not so engaged, the Acquirer must provide MasterCard with "compelling" evidence to that effect.[61] In either case, MasterCard will inform the trademark owner of the result of the investigation by the Acquirer.

If the Acquirer decides to terminate the agreement with the Merchant, the Acquirer must list that Merchant in the MasterCard MATCH[62] (Member Alert to Control High-risk Merchants) program, which is a program that helps Acquirers identify potentially high-risk Merchants before entering into a Merchant agreement. Unlike Visa's policy, if the Acquirer fails to comply with MasterCard's policy, the Acquirer may be removed from membership.[63]

Interestingly, MasterCard's policy is territorial, in that it distinguishes between different jurisdictions: the Acquirer is obligated to suspend or terminate sales by a Merchant only to Customers in countries where the sale of those goods is, in fact, prohibited.[64] If a website is selling, for example, parallel imports which may be allowed in Canada but prohibited in the United States, the Acquirer is not required to terminate the payment services to Customers in Canada. It is unclear how this is done.[65]

(b) Acquirers

Anti-counterfeiting policies are not limited to PNAs. There are some Acquirers who offer — albeit limited — avenues for IP holders to obtain relief for infringement.

---

58 *Ibid.*

59 *Ibid.*

60 *Ibid.*

61 *Ibid.*

62 "MATCH — Help assess risk prior to signing a merchant" online: MasterCard <https://developer.mastercard.com/portal/display/api/MATCH >.

63 MasterCard Anti-Piracy Policy, *supra* note 56 at 3.

64 *Ibid.*

65 The MasterCard policy does not have guidance, although it would be possible to distinguish Canadian Customers from U.S. Customers through their Internet Protocol addresses, or, the Acquirer may require the Merchant to indicate on the webpage that the goods for sale are not available to U.S. Customers.

(i) PayPal

PayPal has a policy to take "appropriate action" to remove PayPal services in connection with infringing material. On its website, PayPal states that IP owners can contact the company if the IP owner has a belief that infringement has occurred or is occurring. An Infringement Report form needs to be filled out and sent to a special email address dedicated for this purpose.[66] There is no information on what Paypal will do with this Infringement Report. Unlike the commitments given by MasterCard above, Paypal does not undertake to create a report of the investigation for the rights holder.[67]

All users of PayPal services, whether Merchant or Customer, must adhere to the Acceptable Use Policy, which states,

> You may not use the PayPal service for activities that:
>
> 1. violate any law, statute, ordinance or regulation,
> 2. relate to transactions involving . . .
>
> (g) items that infringe or violate any copyright, trademark, right of publicity or privacy or any other proprietary right under the laws of any jurisdiction.[68]

It would seem that PayPal could cite violation of clause 2(g) of its Acceptable Use Policy in cases where a Merchant website accepts PayPal payments for counterfeit goods.

(ii) Moneris

There is a template contract that a Merchant signs with Moneris called the Merchant Bankcard Agreement.[69] Nothing in this contract stipulates any acceptable user policy such as that found with PayPal, for example. However, there is a term warning the Merchant that Moneris may, upon written instruction from a PNA, terminate access to that PNA.[70]

(iii) Amazon Payments

Amazon Payments has an "Acceptable Use Policy" that lists items and activities prohibited with their services. Among the list are:

> Illegal, Inappropriate or Offensive Items or Activities — includes any good or service that violates local, state, or federal laws or regulations or that

---

66 "Infringement Report" online: PayPal <https://www.paypalobjects.com/webstatic/en_CA/ua/pdf/infringementreport.pdf>.

67 The rights holder filling out the report must sign the document stating "I understand that this Report may lead to the temporary or permanent restriction of the PayPal account and/or PayPal services associated with the Webpage", *ibid* at 2.

68 "PayPal Acceptable Use Policy" online: PayPal <https://www.paypal.com/ca/webapps/mpp/ua/acceptableuse-full>.

69 "Merchant Bankcard Agreement, Terms/Conditions, OA-008/SA-008", online: E-merchant <https://www.emerchant.com/cms-assets/documents/7540-367101.moneris-merchant-agreement.pdf>.

70 *Ibid* at article 26(B)ii) at 13.

> would be generally offensive to others. Examples include stolen goods, Cuban cigars, cable descramblers, *materials that infringe other's intellectual property rights (including pirated software and counterfeit goods)*, human body parts, endangered species, items that defame or slander others, hate literature, occult materials, and any other items or activities that in our judgment are illegal, inappropriate or offensive in connection with our services.[71]

Consequences of violating the Acceptable Use Policy may include blocking the transaction, suspension of services, or termination of the account of violators.[72] IP rights holders can report violations of this policy by going to the Contact Us page of Amazon Payments.[73]

(iv) eBay

eBay is an online auction website that allows users to buy and sell items online. Although not an Acquirer per se, eBay does own PayPal, and anything purchased using its services must be done through PayPal. There are over 128 million active users, and more than 500 million items listed on eBay.[74]

To facilitate cooperation with IP rights holders, eBay created a program called Verified Rights Owner, or VeRO, which allows IP rights holders to ask eBay to remove listings that offer for sale items infringing on their IP rights.[75] A rights holder with a "good-faith belief" that a listing contained a potentially infringing item could submit a Notice of Claimed Infringement form (or a "NOCI") to inform eBay of the problematic listing.[76] The NOCI must include the following information:

> 1. a signature of the person authorized to act on behalf of the rights holder (could be the attorney or agent);
>
> 2. description of the item in question to which an IP right applies, and identification of that IP rights (e.g. trademark or copyright);
>
> 3. identification of where the alleged infringing material is found on eBay's website;

---

71 "Acceptable Use Policy" (8 February 2014), online: Amazon Payments <https://payments.amazon.com/help/Checkout-by-Amazon/User-Agreement-Policies/Acceptable-Use-Policy> [emphasis added].

72 *Ibid.*

73 "Contact Us", online Amazon Payments <https://payments.amazon.com/contactusinfo>.

74 eBay, "Who We Are", online: eBay <http://www.ebayinc.com/who_we_are/one_company>.

75 eBay, "What is VeRO and why was my listing removed because of it?", online: eBay <http://pages.ebay.com/help/policies/questions/vero-ended-item.html>. Luxury brand owners claim that the VeRO program is not enough. See "Handbagged; eBay's legal woes", *The Economist* 387:8585 (21 June 2008) at 76, although it seemed to be enough for the U.S. courts; see Charles R Macedo, "US trade mark owners must police their own marks on eBay" (2010) 5:7 J Intell Prop L & Prac 484.

76 eBay, "Reporting intellectual property infringements (VeRO)", online: eBay <http://pages.ebay.com/help/tp/vero-rights-owner.html>.

> 4. contact information;
>
> 5. a statement that the person submitting the NOCI (from #1) has a good-faith belief that the use of the material complained of is not authorized by the rights holder; and
>
> 6. a statement that the information in the NOCI is true, and that the Person submitting is either the rights holder or is authorized to act on his or her behalf.[77]

Within twenty-four hours of verifying that the NOCI contains all the required information and has "indicia of accuracy", eBay will remove the challenged listing.[78] Upon removal of the offending listing, eBay will contact the Merchant to inform that the listing was removed and provide relevant information to prevent the Merchant from later committing the same violation.[79] eBay will also periodically review the Merchant's account and may suspend that account if further remedial action is warranted.[80]

A Customer who unwittingly buys a counterfeit good is not necessarily without recourse. Under either eBay's or PayPal's buyer protection plan, the money spent can be reimbursed under certain circumstances, providing that the Customer presents evidence that the item was, in fact, counterfeit.[81] A Merchant whose listing was removed will be directed towards the rights holder's "About Me" page (found within the eBay site) and invited to contact the rights holder directly for more information on why the listing was removed.[82]

(c) Comparison

A comparison of the kinds of anti-counterfeiting policies relied upon by PNAs and Acquirers reveals two different approaches: one more comprehensive, with the possibility of reports (favoured by the PNAs), the other less comprehensive, and more based on the breach of acceptable use policies, as opposed to IP infringement (favoured by the Acquirers).

(i) PNA policies

The policies used by the PNAa (Visa and MasterCard) are quite similar. Since they do not deal directly with the Merchant, any investigations or inquiries must go through the Acquirer. Visa or MasterCard can insist that the Acquirer investigate the accusation of counterfeiting with its Merchant, but neither Visa nor MasterCard can "shut off" the payment access directly. Through contractual relations with the Acquirer, Visa or MasterCard is able to insist that investigations be made, and in the case where the Merchant does not agree to cease selling the goods at issue, or if

---

77 *Ibid.*

78 *Tiffany (NJ) Inc. v. eBay Inc.*, 576 F. Supp. (2d) 463 (SDNY 2008) at 478 [*Tiffany*].

79 *Ibid.* For example, eBay could give evidence of the IP rights that the Merchant was infringing, as well as contact information.

80 *Ibid.*

81 *Ibid.*

82 *Ibid.*

the Merchant does not provide evidence that supports a genuine issue regarding the lawfulness of the Merchant's sale of the goods at issue, Visa or MasterCard can expect the Acquirer to terminate processing credit card payments for the Merchant. In the case where the Merchant offers some evidence of a genuine dispute regarding the lawfulness of the sale of the goods, then Visa or MasterCard will inform the trademark owner and most likely suggest that concerns be addressed directly to the Acquirer or the Merchant. In both cases, the Merchant has an opportunity to respond to these allegations to the Acquirer, who would then bring the response back to the PNA.

(ii) Acquirer policies

By contrast, the policies offered by the Acquirers are not based on whether IP infringements occurred, but rather on breaches of existing "acceptable use policies". PayPal and Amazon Payments will allow IP owners to notify them if payment services were being used to sell counterfeit goods on a website.[83] But there is no follow-up with the IP owner. Regarding the Merchants, it is unclear whether there is a mechanism to respond to any allegations of IP infringement. If PayPal or Amazon Payments discovers that a Merchant has breached a term in the acceptable user policy (e.g. by selling counterfeit goods), the payment services can be shut off. In its user agreement contract, PayPal retains sole discretion in deciding whether a Merchant (or any user) has engaged in "Restricted Activities" (which specifically prohibits the sale of counterfeit goods), which could result in the withdrawal of their services.[84]

Although eBay's VeRO program is similar to the anti-counterfeiting policies of Visa or MasterCard regarding the information requested, where Visa and MasterCard simply pass on the information, eBay will shut down the listing immediately.[85] Also, Visa and MasterCard take much more of an "arm's length" approach, simply passing along information to the corresponding Acquirers. eBay takes more direct action, perhaps in its capacity of acting more like an Acquirer than a PNA.[86]

(d) Voluntary Systems

All of these systems are voluntary in the sense that there are no statutory or regulatory requirements for these companies to look into every instance of counterfeiting. Since Visa and MasterCard both have a vested interest in ensuring that their brand does not obtain a reputation for being involved in illegal activities ("Visa — the online payment service preferred by most counterfeiters®"), it makes sense that the companies create procedures to help shut down online counterfeiting. In a recent interview, Colm Dobbyn, head of IP at MasterCard Worldwide, stated that the

---

83 It does not seem that Moneris has a procedure for an IP rights holder to make a claim directly.

84 "PayPal User Agreement", online: PayPal, Inc. <https://www.paypal.com/ca/webapps/mpp/ua/useragreement-full>.

85 *Tiffany*, *supra* note 78.

86 The court found that eBay has dedicated many resources towards anti-counterfeiting initiatives, including $20 million annually and two hundred employees dedicated to combating infringement on its site. *Tiffany*, *supra* note 78 at 476.

company's anti-counterfeiting initiative was developed over a number of years and, "We want our brand to be trusted and therefore certainly do not want to have it associated with illegal or other questionable activities."[87]

This begs the question: is there a place for government to require, by law, online payment services to investigate accusations of trademark counterfeiting?

IV. GOVERNMENTAL POLICY OPTIONS

(a) Prioritizing IP Rights

Since the signing of TRIPs, countries have been giving IP rights a higher priority as evidenced by the inclusion of IP-specific chapters in multi-lateral and bi-lateral agreements.[88] The same holds true for domestic legislation, as evidenced by the numerous initiatives where the Canadian Government has addressed IP rights and their enforcement in recent years:

- In 2007, two Parliamentary Standing Committee reports independently confirmed the importance of fighting counterfeiting and piracy.[89]
- In 2012, the *Copyright Modernization Act*[90] was given Royal Assent.[91]

---

87 Sara-Jayne Clover, "Inside Track: Mastercard", *World Trademark Review* 44 (Aug/Sept 2013) 15 at 16.

88 Members of WIPO have negotiated several IP-specific treaties, including the *WIPO Copyright Treaty*, 20 December 1996, 2186 UNTS 121 (entered into force 6 March 2002), online: WIPO <http://www.wipo.int/wipolex/en/wipo_treaties/text.jsp?file_id=295157>, the *WIPO Performances and Phonograms Treaty*, 20 December 1996, 2186 UNTS 203 (entered into force 20 May 2002), online: WIPO <http://www.wipo.int/wipolex/en/wipo_treaties/text.jsp?file_id=295477>, the *Singapore Treaty on the Law of Trademarks*, 27 March 2006, (entered into force 16 March 2009), online: WIPO <http://www.wipo.int/wipolex/en/wipo_treaties/text.jsp?file_id=290013> [Singapore Treaty], the *Beijing Treaty on Audiovisual Performances*, 24 June, 2012, online: WIPO <http://www.wipo.int/wipolex/en/wipo_treaties/text.jsp?file_id=295838>, and the *Marrakesh Treaty to Facilitate Access to Published Works for Persons Who Are Blind, Visually Impaired or Otherwise Print Disabled*, 28 June 2013, online: WIPO <http://www.wipo.int/wipolex/en/wipo_treaties/text.jsp?file_id=30101>. For a more comprehensive list, see "WIPO-Administered Treaties", online: WIPO <http://www.wipo.int/wipolex/en/wipo_treaties/>.

89 House of Commons, Standing Committee on Industry, Science and Technology (INDU), "Counterfeiting and Piracy are Theft" (June 2007) (Chair: James Rajotte); House of Commons, Standing Committee on Public Safety and National Security, "Counterfeit Goods in Canada — A Threat to Public Safety" (May 2007) (Chair: Gary Breitkreuz).

90 Canada Bill C-11, *An Act to amend the Copyright Act*, 1st Sess, 41st Parl, 2011 (given Royal Assent 29 June 2012) [CMA].

91 Along with allowing Canada to implement the WIPO Internet treaties and providing for legal protection for digital locks, the *Copyright Modernization Act* clarified the roles and responsibilities of Internet Service Providers (ISPs) and search engines.

- In 2013, the government introduced Bill C-56[92] (now Bill C-8[93]), which addressed many of the recommendations in the earlier Parliamentary reports dealing with counterfeiting and piracy (particularly at the border). The second part of budget implementation, which contains amendments related to the other two IP treaties mentioned above, was tabled in October 2014.[94]
- Another Committee report[95] released in March 2013 contained similar recommendations regarding IP enforcement, which were generally covered under Bill C-8.[96]
- In January 2014, the Government tabled five international treaties related to IP.[97]
- In June 2014, the *Economic Action Plan 2014 Act, No. 1*,[98] which contained amendments related to three of the IP treaties mentioned above, received Royal Assent.

Although none of the above initiatives specifically include PNAs or their regulation, given this interest in anti-counterfeiting initiatives, and considering that laws in the virtual world should mirror those in the real world, policy makers may wish to consider some options regarding the role of PNAs in the fight against online counterfeiting.

---

92 Canada Bill C-56, *An Act to amend the Copyright Act and the Trade-marks Act and to make consequential amendments to other Acts*, 1st Sess, 41st Parl, 2013, (first reading 01 March 2013).

93 Canada Bill C-8, *An Act to amend the Copyright Act and the Trade-marks Act and to make consequential amendments to other Acts*, 2nd Sess, 41st Parl, 2013, (third reading 02 October 2014) [*Combating Counterfeit Products Act*].

94 Canada Bill C-43, A second Act to implement certain provisions of the budget tabled in Parliament on February 11, 2014 and other measures, 2nd Sess, 41st Parl, 2014 (first reading 23 October 2014).

95 House of Commons, INDU, "Intellectual Property Regime in Canada" (March 2013) (Chair: David Sweet) at 52. While the report restated many of the recommendations in the 2007 Reports on counterfeiting and piracy, nothing in this report suggested legislating obligation on PNAs.

96 Canada, "Government Response to the Third Report of the House of Commons Standing Committee on Industry, Science and Technology, '*Intellectual Property Regime in Canada*'" 41st Parl, 1st Sess, (June 2013), online: Parliament of Canada <http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=6237704&Language=E&Mode=1&Parl=41&Ses=1>.

97 Neil Melliship, "Canadian Government Tables 5 IP Treaties in the House of Commons", *Canadian Trademark Blog* (28 January 2014), online: Canadian Trademark Blog <http://trademarkblog.ca/canadian-government-tables-5-ip-treaties-house-commons/>.

98 Canada Bill C-31, *An Act to implement certain provisions of the budget tabled in Parliament on February 11, 2014 and other measures*, 2nd Sess, 41st Parl, 2014 (given Royal Assent 19 June 2014).

(b) Option 1 — Status Quo

One option, as always, is to maintain the status quo, thus allowing the courts to handle issues as they come up. In Canada, for example, there are existing mechanisms where website Merchants dealing in counterfeit goods can be made to pay damages or forced to shut down.

(i) Civil remedies in the Trade-marks Act

The TMA allows courts broad discretion to give remedies:

> Where a court is satisfied, on application of any interested person, that any act has been done contrary to this Act, *the court may make any order that it considers appropriate in the circumstances*, including an order providing for relief by way of injunction and the recovery of damages or profits and for the destruction, exportation or other disposition of any offending wares, packages, labels and advertising material and of any dies used in connection therewith.[99]

Courts have used this provision in many counterfeiting cases to provide punitive damages and even compensatory damages (akin to statutory damages).[100] It may simply be a matter of time before courts become more comfortable with e-commerce such that these types of injunctions and court orders will become more prevalent. It may therefore be premature to begin imposing new statutory requirements on judges.[101]

(ii) Law enforcement

Government agencies in the U.S. already have broad powers to shut down websites offering to sell infringing goods. In the past several years, U.S. enforcement agencies have been operating a crackdown coinciding with "Cyber Monday", the Monday after the American Thanksgiving holiday when retailers offer online

---

99 TMA, *supra* note 30 s 53.2 [emphasis added].

100 See *Oakley Inc. v. Jane Doe*, 2000 CarswellNat 5990, 193 F.T.R. 42, 2000 CarswellNat 1995 (Fed. T.D.), at para 3, where the court assessed compensatory damages of $3,000 in the case of defendants operation from temporary premises, $6,000 from conventional retail premises, and $24,000 against manufacturers and distributors of counterfeit goods. More recent cases have increased those amounts, see *Harley-Davidson Motor Co. Group LLC v. Manoukian*, 2013 FC 193, 2013 CarswellNat 449 (F.C.) at para 45; *Guccio Gucci S.p.A. v. Mazzei*, 2012 CarswellNat 1403, 101 C.P.R. (4th) 219, 2012 CarswellNat 994, 2012 FC 404 (F.C.) at para 43; *Louis Vuitton Malletier S.A. v. Yang*, 2007 CarswellNat 5591, 62 C.P.R. (4th) 362, 2007 CarswellNat 3923 (F.C.) at para 43.

101 There is at least one Canadian case where the court enjoined a defendant from offering for sale online goods that bore the plaintiff's trademark. In *LifeGear Inc. v. Urus Industrial Corp.*, 2004 CarswellNat 2190, 29 C.P.R. (4th) 441, 2004 CarswellNat 120, 2004 FC 21 (F.C.); affirmed 2005 CarswellNat 2015, 38 C.P.R. (4th) 507, 2005 CarswellNat 456, 2005 FCA 63 (F.C.A.), which dealt with an order for contempt of court, the judge found that the defendant failed to comply with an order to cease infringing the plaintiff's registered trademark by continuing to "offer those products for sale through its website".

sales that complement the in-store sales found during "Black Friday". As part of this initiative in 2010, the U.S. Department of Justice and Department of Homeland Security's Immigration and Customs Enforcement (ICE) agency obtained court orders to shut down eighty-two websites accused of selling infringing goods.[102] Similar crackdowns were conducted in 2011[103] and 2012.[104] For the last Cyber Monday in 2013, a joint effort with non-U.S. law enforcement agencies resulted in the seizure of over 700 domain names associated with the sale of counterfeit goods.[105] A visit to one of the seized domain names brings up a government notice[106] saying that the domain name has been seized by ICE-Homeland Security Investigations pursuant to a seizure warrant.[107]

Although the RCMP has not been involved in the shutting down of any website for counterfeiting, there has been at least one criminal case where a website was shut down and assets seized. In 2013, the RCMP raided $2.5 million in cash from a gambling ring with ties to Hells Angels.[108] The seizure included two domain names hosting the gambling sites; <PlatinumSB.com> and <Betwho.com>, which were registered in Costa Rica.[109]

(iii) Existing anti-counterfeiting policies

As mentioned above in section III, many PNAs and Acquirers already have voluntary policies in place for IP owners to seek redress for the online sale of counterfeit goods. There has not been a huge clamor for legislative change in this area domestically or internationally, either from PNAs or stakeholders, nor were such changes mentioned in the Canadian Committee Reports.

---

102 Grant Gross, "Courts Shut Down 82 Sites for Alleged Copyright Violations", *PCWorld* (29 November 2010) online: PCWorld <http://www.pcworld.com/article/211832/article.html>.

103 Ernesto, "Feds Seize 130+Domain Names in Mass Crackdown", *TorrentFreak* (25 November 2011) online: TorrentFreak <http://torrentfreak.com/feds-seize-130-domain-names-in-mass-crackdown-111125/>.

104 Timothy B. Lee, "Feds seize 101 domains for counterfeiting in 'Cyber Monday' operation", *Ars Technica* (26 November 2012) online: Ars Technica <http://arstechnica.com/tech-policy/2012/11/feds-seize-101-domains-for-counterfeiting-in-cyber-monday-operation/>.

105 Faye DeHoff, "Hundreds of domain names selling counterfeit products seized by ICE", *KVOA* (2 December 2013), online: KVOA <http://www.kvoa.com/news/hundreds-of-domain-names-selling-counterfeit-products-seized-by-ice/>.

106 For an example, see <http://closetkicks.com/>, one of the domain names seized in the 2013 raid.

107 These warrants are obtained pursuant to 18 USC §981(general civil forfeiture) or §2323 (civil forfeiture resulting from the trafficking of counterfeit goods).

108 Adrian Humphreys, "RCMP charge six men, seize $2.5M in cash after multiple raids in connection with 'Mafia-linked' illegal gambling ring", *The National Post* (5 February 2013), online: The National Post <http://news.nationalpost.com/2013/02/05/glitzy-super-bowl-gala-turned-gang-takedown-rcmp-bust-illegal-gambling-ring-with-alleged-ties-to-hells-angels-mafia/>.

109 *Ibid.*

(iv) Contributory infringement

Although the concept of contributory infringement by an intermediary has yet to find its path in Canadian trademark law, it has been considered in other countries. The U.S. Supreme Court found that in order to find contributory infringement, there has to be knowledge that the person to whom the goods are supplied (or services are used) is engaged in trademark infringement.[110] This test was applied in the context of e-commerce. In *Tiffany (NJ) Inc. v. eBay Inc.*, a U.S. case involving the sale of counterfeit goods on eBay, the Second Circuit appellate court found that the website was neither liable for any trademark infringement, nor responsible to police the different sales.[111] In particular, the court found that for a service provider to be liable there must be more than a "general knowledge" that its service is being used to sell counterfeit goods.[112]

There have also been a couple of U.S. cases dealing directly with PNAs and contributory infringement. In one case, the court dismissed the secondary copyright and trademark infringement claims, noting that the PNA (here, Visa) lacked direct control and monitoring.[113] However, another case found liability with a sales organization that aided the Merchant with its website that was used to sell counterfeit goods.[114] The latter case could be distinguished from the earlier case since all the players involved were members of the acquiring industry, as opposed to being strictly PNAs.[115] If a similar case were brought in front of a Canadian court, the judge could make use of these U.S. cases for guidance, and may find, in the circumstances, contributory infringement.

(c) Option 2 — Legislative Changes

Countries could also opt for legislative changes that would explicitly require PNAs to investigate allegations of counterfeiting on websites using their services. Such measures were recently attempted in the U.S.,[116] but have since been shelved. Policy makers would have to consider several factors.

---

110 *Inwood Laboratories, Inc. v. Ives Laboratores Inc.*, 456 U.S. 844 (1982).

111 600 F.3d 93 (2d Cir, 2010).

112 *Ibid* at 107.

113 *Perfect 10, Inc. v. Visa International Service Ass'n*, 494 F.3d 788 (9th Cir, 2006).

114 *Gucci America, Inc. v. Frontline Processing Corp*, 721 F.Supp (2d) 228 (SDNY, 2010).

115 Kelly K Yang, "Paying for Infringement: Implicating Credit Card Networks in Secondary Trademark Liability" (2011) 26 Berk Tech LJ 687 at 715.

116 Two U.S. Bills, US, Bill HR 3261, *Stop Online Piracy Act*, 112th Cong, 2011 [SOPA], and US, Bill S 969, *Preventing Real Online Threats to Economic Creativity and Theft of Intellectual Property Act of 2011*, 112th Cong, 2011 [PIPA] both required PNAs to investigate allegations of counterfeiting and piracy on websites using their services. Other provisions in these bills were opposed both by major Internet companies (Declan McCullagh, "Google, Facebook, Zynga oppose new SOPA copyright bill", *CNET* (15 November 2011) online: CNET <http://news.cnet.com/8301-31921_3-57325134-281/google-facebook-zynga-oppose-new-sopa-copyright-bill/>), and the White House (Victoria Espinel, Aneesh Chopra, and Howard Schmidt, "Combating Online Piracy while Protecting an Open and Innovative Internet" (14 January 2012) online: The

(i) Controversy

The public reaction to SOPA and PIPA was massive. Some websites called it the "largest online protest in history"[117] with reportedly thousands of websites having joined in on the protest,[118] including Wikipedia, Google, Mozilla, Reddit, and WordPress.[119] Therefore, it could be expected that the mere mention of SOPA-like provisions moving into any country's legislation would bring about its own set of protests. Judging by the number of articles linking the *Combating Counterfeit Products Act* to ACTA, and also to SOPA and PIPA, to say that legislating in the area has "sensitivities" could be an understatement.[120]

(ii) PNAs as intermediaries

Considering the type of contractual relationships that PNAs like Visa and MasterCard have, it is doubtful that they would have anything more than a "general knowledge" that their services are being used for counterfeiting, particularly since these PNAs do not deal directly with the owners of the counterfeit websites. By introducing possible liability for PNAs in legislation, there is a risk that the government would be changing the status quo and possibly upsetting an existing balance.

Given that the *Copyright Modernization Act* exonerates Internet Service Providers and search engines from liability to the extent that these were acting as neutral intermediaries and participating in the created "notice and notice" regime,[121] it can

---

White House <https://petitions.whitehouse.gov/response/combating-online-piracy-while-protecting-open-and-innovative-internet>) leading to both bills being taken off the table. It did not help matters that the *Anti-Counterfeiting Trade Agreement*, 1 October 2011, 50 ILM 239 (not yet entered into force) [ACTA] was being signed roughly the same time, resulting in increased public sensitivity to *any* IP initiative. For more on ACTA, please see See Kenneth L Port, "A Case Against the ACTA" (2011) 33:3 Cardozo L Rev 1131, and Kimberlee Weatherall, "Politics, Compromise, Text and the Failures of the *Anti-Counterfeiting Trade Agreement*" (2011) 33:2 Sydney L Rev 229.

117 "Victory!", online: SOPAStrike <http://sopastrike.com/>.

118 "Internet Blackout: 7,000 Sites Join Wikipedia", *Deadline* online: Deadline <http://www.deadline.com/2012/01/wikipedia-blackout-pipa-sopa-protest-google/>.

119 Zach Carter, "Google Joins Online SOPA Protest", *The Huffington Post* (17 January 2012), online: Huffington Post <http://www.huffingtonpost.com/2012/01/17/google-joins-online-sopa-protest_n_1210990.html>.

120 Ben Rawluck, "That's so fake: Canada's new counterfeiting laws are designed to restrict rights and make big business happy", *This Magazine* 47:1 (July-August 2013) at 12; Josh Tabish, "How New ACTA Internet Lockdown Measures Are Coming to Canada", *Open Media* (13 March 2013), online: Open Media <https://openmedia.ca/blog/how-new-acta-internet-lockdown-measures-are-coming-canada>; BCLaraby, "So you want to stop Bill C-8 (ACTA)" (4 December 2013), online: Reddit <http://www.reddit.com/r/canada/comments/1s2u1q/so_you_want_to_stop_bill_c8_acta_xpost_from/>; Cory Doctorow, "ACTA about to be quietly written into Canadian law", *Boing Boing* (3 December 2013), online: Boing Boing <http://boingboing.net/ 2013/12/03/acta-about-to-be-quietly-writt.html>.

121 Government of Canada, "What the *Copyright Modernization Act* Means for Internet Service Providers, Search Engines and Broadcasters", online: Balanced Copyright <http://www.ic.gc.ca/eic/site/crp-prda.nsf/eng/rp01188.html>.

be argued that there is no expectation to have intermediaries "police" the Internet. Putting new obligations on PNAs may run the risk of creating some unintended results such as courts finding that any PNA taking an interest in preventing counterfeiters from using their services would no longer be "neutral".

(iii) Jurisdiction

The U.S. is in a unique position to regulate Internet activities since virtually all website and domain name hosts are based within their territory. The three largest generic top-level domains (gTLDs), dot-com, dot-org, and dot-net, are managed by U.S.-based domain name registries.[122] This is why the U.S. was able to designate any domain name as a "domestic domain name" so long as the domain name is "registered or assigned by a domain name registrar, domain name registry, or other domain name registration authority, that is located within a judicial district of the United States".[123] Regardless of where the registrant of a domain name actually resides, that domain name could be deemed to be a "domestic domain name" and U.S. courts could exercise jurisdiction.[124]

Regulation for non-U.S. countries can be more complicated. Take the situation where the website in question resides in a server in the U.S. A country introducing provisions compelling the PNAs to investigate foreign websites may be confronted with jurisdiction issues. How effective would such legislative provisions be if the PNAs routinely ignored these court orders? It may end up being simpler for rights holders to go to where the server resides (i.e. the U.S.) to seek remedies, which would incur other expenses for litigation.[125]

(iv) Minimal results

Even if legislative options were successful, and websites were being taken down and the domain names seized, it is still very easy for that website owner to

---

122 Dot-com and dot-net are managed by Verisign, while dot-org is managed by the Public Interest Registry. See Internet Corporation for Assigned Names and Numbers (ICANN), "Registry Agreements", online: ICANN <http://www.icann.org/en/about/agreements/registries> for the individual registry agreements.

123 SOPA, *supra* note 116 at s 101(3).

124 Michael Geist, "U.S. could claim millions of Canadian domain names in piracy battle", *The Toronto Star* (13 November 2011) online: Toronto Star <http://www.thestar.com/business/2011/11/13/geist_us_could_claim_millions_of_canadian_domain_names_in_piracy_battle.html>.

125 There may be some room for other countries to legislate over websites registered in their country-code domain name space (ccTLD), if the rules provide for sufficient presence requirements. For example, registrants of a domain name in the dot-ca domain name space must establish some sort of Canadian presence by showing that the registrant is a Canadian citizen, or a business incorporated under Canadian laws. If a website with a dot-ca domain name was selling counterfeit goods, then it is probable that the Merchant's Acquirer and PNA also have a Canadian presence, and would therefore be subject to a Canadian court order. However, this solution is limited because would-be counterfeiters could simply by-pass the dot-ca space and opt for the non-regulated ones like dot-com.

start up a new website with a new domain name for its counterfeiting operations. It is very inexpensive for a website owner to obtain and register a new domain name.[126] It would not be difficult to obtain a new Acquirer if necessary, even if the website owner needed to incorporate a new numbered business. PNAs do not contract directly with Merchants, so these companies may not be aware of prior court orders against a certain Merchant.

Although U.S. enforcement agencies shut down and seized over 700 domain names and websites last year, new websites devoted to the sale of counterfeit goods continue to pop up. The sites seized by the RCMP mentioned above were back up within hours.[127]

(d) Option 3 — Create Industry Guidelines

Considering that PNAs such as Visa and MasterCard already have policies to deal with counterfeiting, perhaps another option is to work with these companies to create industry guidelines based on these existing policies. This may be an opportune time for such, as there seems to be movement within the industry itself to find ways to cut off payment services to websites involved in counterfeiting or piracy.[128] Trademark owners would certainly welcome some harmonization among these policies so that they would not have to create different enforcement plans for each type of payment service. This could also be an opportunity for Acquirers to adopt similar policies that would work in tandem with the PNAs.

There is precedent for government leadership in creating guidelines in the field of e-commerce. The *Canadian Code of Practice for Consumer Protection in Electronic Commerce* lists eight principles that would be considered "good practice benchmarks" for Merchants engaging in e-commerce.[129] For example, one of the principles underlines the social responsibility Merchants have to determine whether the Customer is a minor and to take "all reasonable steps to prevent monetary transactions" with minors.[130] These guidelines were "endorsed" by federal, provincial, and territorial ministers responsible for consumer affairs in 2004.[131]

---

126 One-year terms for dot-ca domain names can go for $39, see online: Canadian Domain <http://www.canadiandomain.ca/pricing.html>; but other websites offer much lower one-year terms registration fees, see online: GoDaddy.com <http://ca.godaddy.com/domains/search.aspx?ci=2629>.

127 Adrian Humphreys, "Betting ring hit with dramatic Super Bowl Sunday raid back up within hours", *The National Post* (6 February 2013), online: The National Post <http://news.nationalpost.com/2013/02/06/betting-ring-hit-with-dramatic-super-bowl-sunday-raid-back-up-within-hours/>.

128 Brad Reed, "Google working with Visa, Mastercard, PayPal to cut off funding for alleged piracy sites", *BGR* (19 February 2013), online: BGR Media <http://bgr.com/2013/02/19/google-anti-piracy-plan-331472/>.

129 Government of Canada, "Consumer Measures Committee" (09 May 2011), online: CMC Web <http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00064.html>.

130 *Ibid* at Principle 8.1.

131 *Ibid.* Here, "endorsed" does not mean that the endorser meets the terms of the guidelines, only that the endorser agrees that the guidelines represent good practice benchmarks for those engaged in e-commerce.

Even though these guidelines were not binding, the Canadian experience of drafting the e-commerce guidelines was a massive project. A working group consisting of not only the federal government, but representatives of provincial governments and other interested organizations was created in 1999.[132] An approval in principle was not achieved until 2003. Questions of jurisdiction come up again, but this time from the federal-provincial angle. Although trade and commerce, and intellectual property, come under the federal powers, regulation of an industry comes under provincial powers.[133]

Efforts to harmonize business practices in Canada must take into account the scope of the federal powers. In the area of securities regulation, efforts to harmonize the current patchwork of provincial regulations started in the 1960s.[134] More recently, in 2008, a panel was appointed to study and provide recommendations, which were published the next year.[135] The panel found that the current system was too inefficient and incongruent to respond to national or international crises, and recommended the creation of a single, national securities regulator.[136] In response, the federal government drafted the *Canadian Securities Act*,[137] which would create a regulatory body empowered to not only perform all the functions currently undertaken by the provincial regulators, but also other functions relating to risk in national capital markets and to securities data collection. The draft legislation was referred to the Supreme Court for its opinion on whether the legislation fell within the federal trade and commerce power. In a unanimous decision, the Court held that the proposed *Canadian Securities Act* would not be valid under the general brand of the federal trade and commerce power.[138]

Although a complete constitutional analysis of any possible federal scheme involving PNAs is beyond the scope of this article, it can be assumed that any

---

132 For a list of organizations involved in the working group, see Government of Canada, "Archived — appendix 1: Working Group on Electronic Commerce and Consumers", online: CMC Web <http://cmcweb.ca/eic/site/cmc-cmc.nsf/eng/fe00074.html>.

133 *Constitution Act, 1867* (UK), 30 & 31 Vict, c 3, ss 91-92, reprinted in RSC 1985, App II, No 5.

134 Canada, *Report of the Royal Commission on Banking and Finance* (Ottawa: Queen's Printer, 1964) and Ontario, *Report of the Attorney General's Committee on Securities Legislation in Ontario* (Toronto: Queen's Printer, 1965).

135 Department of Finance, News Release, 2008-018, "Government of Canada Appoints Expert Panel to Review Securities Regulation" (21 February 2008).

136 Canada, Expert Panel on Securities Regulation, *Final Report and Recommendations* (Ottawa: Department of Finance, 2009).

137 The Bill was never tabled in the House of Commons, but an archived version can be found here: <http://www.fin.gc.ca/drleg-apl/csa-lvm-eng.htm>.

138 *Reference re Securities Act (Canada)*, [2011] 3 S.C.R. 837, 2011 CarswellNat 5244, 2011 CarswellNat 5243, 2011 SCC 66 (S.C.C.). Not everyone agreed with the finding. See Malcolm Lavoie, "Understanding 'Trade as a Whole' in the *Securities Reference*" (2013) 46:1 UBC L Rev 157; Wayne Gray and Stephen Genttner, "Supreme Court's unanimous ruling sinks Canadian *Securities Act* (but leaves much to be salvaged)" (23 December 2011), online: McMillan <http://www.mcmillan.ca/Supreme-Courtss-Unanimous-Ruling-Sinks-Canadian-Securities-Act-But-Leaves-Much-to-be-Salvaged>.

initiative to create binding national guidelines or regulations that involve the trade and commerce power would be, at best, a complicated endeavor.[139]

V. CONCLUSION

Counterfeiting is a serious problem, and one that brings new challenges in the online sphere. Figures on the cost of seizures of counterfeits are extremely high. The RCMP has released data showing a yearly increase in the number of occurrences involving harmful counterfeit goods, as well as an increase in the total retail value of seizures of counterfeits.[140] The European Commission stated that €1 billion worth of fake goods were seized at EU borders,[141] while U.S. figures show seizures of $1.26 billion.[142] Although damage awards in trademark counterfeiting cases have been increasing,[143] and other cases are including injunctions against selling or offering to sell counterfeit goods online,[144] the courts are still grappling with how to apply trademark principles to online activities. It is particularly difficult for trademark owners to enforce their rights against websites where the owner is outside the jurisdiction, or is simply unable to be found. Solutions to the problem of online counterfeiting may require more than simple trademark enforcement actions.

We have seen the role that Payment Network Associations such as Visa and MasterCard play in facilitating e-commerce. These networks provide the means for Consumers to purchase goods online from Merchants quickly and easily. Without these networks, Merchants would have to seek more traditional ways to obtain payments, for example, through money orders or checks sent in the mail. One of the reasons that e-commerce is attractive is because of the speed and efficiency with which payments can be made, i.e. the ability to process payments electronically. The lack of access to electronic payment networks would run counter to the benefits that the speed and efficiency of e-commerce websites bring. Since PNAs have created the networks that allow counterfeiters to sell goods online, and provide the

---

139 Although "banks and banking" are one of the federal powers, PNAs are not banks, but technology companies that oversee networks. There may be an argument that they are acting like banks, but there is also an argument that regulation of them would be regulation of an industry (a provincial power).

140 RCMP, "2012 Intellectual Property (IP) Crime Statistics" (last modified 20 February 2013), online: RCMP <http://www.rcmp-grc.gc.ca/fep-pelf/ipr-dpi/report-rapport-2012-eng.htm>.

141 European Commission, News Release, "Protecting Intellectual Property Rights: Customs detain €1 billion worth of fake goods at EU borders in 2012" (5 August 2013), online: Europa <http://europa.eu/rapid/press-release_IP-13-761_en.htm?locale=en>.

142 U.S. Customs and Border Protection, News Release, "CBP, HIS Announce Fiscal Year 2012 Intellectual Property Rights Seizure Statistics" (17 January 2013), online: CBP <http://www.cbp.gov/newsroom/national-media-release/2013-01-17-050000/cbp-hsi-announce-fiscal-year-2012-intellectual>.

143 For example, in *Louis Vuitton Malletier S.A. v. Singga Enterprises (Canada) Inc.*, 2011 CarswellNat 2317, 2011 CarswellNat 3020, 2011 FC 776 (F.C.), involving both copyright and trademark infringement, the judge ordered damages of $2.48 million.

144 *Lifegear*, *supra* note 101.

"life blood" for these websites to function, it would make sense to require PNAs to cease providing payment services to websites devoted solely to the sale of counterfeit goods. But upon further study, such obligations may not be so easily created.

It turns out that the power these PNAs possess is more indirect than direct. PNAs manage the electronic payments conducted online through their networks, yet these companies have little control over the day-to-day operations of the Merchants who are doing the actual selling. The power held by the PNAs comes from the contractual relations they have with the financial institutions (the Acquirers) who, in turn, deal directly with these Merchants. The only "power" PNAs have is to require these Acquirers to investigate allegations of wrongdoing. The question then becomes whether regulations ought to require PNAs to use this power over the Acquirers.

Any attempt by governments to force PNAs to use this power over Acquirers would be controversial. Not only have we witnessed an Internet uprising in response to recent U.S. attempts to legislate in this area, but there are increased sensitivities in the public sphere regarding any changes to intellectual property laws. Questions of jurisdiction come up as well, since this power stems from contractual law as opposed to intellectual property. Also, any legislative solution would need to involve the United States, since most of the Internet domain names and websites flow through that jurisdiction.

Simply because an initiative would be difficult, does not mean it is not worth pursuing. A compromise position between the status quo and government legislation is a voluntary code. Canada could bring together various PNAs and Acquirers to find a "made-in-Canada" solution. Or on a grander scale, different countries could come together to create some "soft law" documents that would outline best practices.[145] PNAs have a vested interest in ensuring their services and networks are not used by counterfeiters, as shown by their current policies. It would be of tremendous help to IP owners if those policies could be more consistent.

---

145 WIPO provides several "soft law" models, such as the Joint Recommendation Concerning Provisions on the Protection of Well-Known Marks (1999), online: WIPO <http://www.wipo.int/export/sites/www/freepublications/en/marks/833/pub833.pdf>, and the Joint Recommendation Concerning Trademark Licenses (2000), online: WIPO <http://www.wipo.int/export/sites/www/freepublications/en/marks/835/pub835.pdf>. Although considered to be optional on their own, the Joint Recommendation on well-known marks has been referred to various trade agreements (see U.S.-Singapore Free Trade Agreement, online: USTR <http://www.wipo.int/export/sites/www/freepublications/en/marks/835/pub835.pdf>, Article 16.1(2)(b)), and several provisions in the Joint Recommendation on licenses are now part of the Singapore Treaty.