WASHINGTON JOURNAL OF LAW, TECHNOLOGY & ARTS
VOLUME 8, ISSUE 1 SUMMER 2012

FINDING SAFE HARBOR: NAVIGATING WASHINGTON'S NEW UNFAIR COMPETITION LAW

Daniel Shickich[*]

CITE AS: 8 WASH. J.L. TECH. & ARTS 1 (2012)
http://digital.law.washington.edu/dspace-law/handle/1773.1/1152

ABSTRACT

Under a new law, manufacturers and retailers that sell products in Washington State could face stiff penalties if their products are made using stolen or misappropriated information technology ("stolen IT"). In 2011 the Washington Legislature passed Substitute House Bill 1495, creating a new cause of action that allows private plaintiffs or the state attorney general to seek injunctive relief and damages against manufacturers that use stolen IT in their business operations. The law also creates an additional claim for actual damages of up to $250,000 against third parties who contract with violating manufacturers and sell the products in Washington. Using unfair competition law to address problems of piracy and infringement is a novel and unproven approach; it remains to be seen how companies will use the law, and how effective the law will prove in changing the behavior of manufacturers and their third-party business partners. This Article explores the legislative history and operation of the new Washington law, including the requirements for liability and "safe harbors" shielding businesses from enforcement. This Article also considers possible federal preemption

---

[*] Daniel Shickich, University of Washington School of Law, Class of 2013. Thank you to Professors Mary Fan and Zahr Said of the University of Washington School of Law and student editor Parker Howell for the assistance and insight.

challenges based on the law's potential overlap with copyright law and federal commerce powers.

TABLE OF CONTENTS

INTRODUCTION

American companies have long complained about the costs of intellectual property ("IP") piracy abroad, particularly in countries such as China and India. Much attention to potential remedies for piracy has focused on the federal level. However, the Washington Legislature in 2011 passed a law aimed at giving domestic businesses a remedy against overseas IP infringement through unfair competition law—a novel approach recently proposed in several other states but passed only in Washington State. Substitute House Bill 1495, codified as Wash. Rev. Code 19.330 ("the Act"), creates a new cause of action allowing private plaintiffs or the state attorney general to seek damages and injunctive relief against a manufacturer of products sold in Washington that makes the goods while using stolen or misappropriated information technology ("stolen IT")—proprietary hardware or software technology that can be owned or licensed. This approach focuses on the harm done to competing businesses when a manufacturer uses stolen IT as part of its business operations. The term "business operations" is broadly defined to include the manufacture, distribution, marketing, or sales of a product.

While the Act's primary target is foreign manufacturers engaged in large-scale IT piracy, it could potentially affect third parties doing business in Washington. A violating manufacturer's products in Washington, whether intended for immediate sale or incorporation into a third-party business's end product, are potentially subject to an injunctive order and attachment. In addition, if a violating manufacturer either fails to appear or has insufficient attachable assets in Washington to satisfy a judgment, a provision in the law allows the plaintiff to seek actual damages against certain third-party businesses operating in Washington that contract with the violating manufacturer. Thus, the Act could disrupt third-party supply chains and subject third-party businesses to liability of up to $250,000. For the unprepared business, the Act could increase legal costs and embroil the company in litigation.

While the Act creates new obligations and possible liability for third-party businesses that contract with violating manufacturers, third-party businesses may largely avoid liability through the use of a number of safe harbor provisions, including simply sending a

letter to the manufacturer demanding proof of compliance with the Act. A third-party business may further minimize any detrimental effect on business processes and avoid ongoing legal costs through changes to contracts and supply chain management practices. For example, a third-party business should implement a code of conduct with all manufacturers that explicitly prohibits use of stolen IT and provides for periodic auditing.

This Article examines the legislative history and operation of the Act, particularly the requirements for finding liability and the safe harbors shielding businesses from enforcement. In addition, this Article introduces possible federal preemption challenges based on the law's potential overlap with federal commerce powers and copyright law.

I. HISTORY AND PASSAGE OF S.H.B. 1495

The Washington Legislature passed the Act against the backdrop of vocalized concerns from Microsoft Corp. and other international businesses regarding the detrimental effect that software piracy has on competition in the state.[1] During legislative committee hearings and floor debate, proponents tied rampant piracy in certain regions abroad, such as China and India, to job loss in Washington, particularly in the technology industry. Supporters argued that by requiring accountability for both manufacturers and third parties, the Act simply demands fairness from manufacturers and their domestic contractual partners. Opponents countered that the Act is overly broad and ambiguous, will increase liability and supply-chain costs by forcing industry to police manufacturers, and could lead to frivolous litigation and abuses of the discovery process.

The Act passed with substantial support in both legislative bodies and became effective on July 22, 2011.[2] A court may not

---

[1] *See, e.g.*, Manuel Valdes, *Piracy Bill Pits Microsoft Against Tech Giants*, KOMONEWS.COM, Mar. 13, 2011, http://www.komonews.com/news/microsoft/117898824.html.

[2] On February 2, 2011, the Washington State House of Representatives passed S.H.B. 1495 by a vote of 90-4. The Washington State Senate then passed an amended version of S.H.B. 1495 by a vote of 39-8 on April 4, 2011. The

award damages against a third party until 18 months from the effective date, or January 22, 2013.[3] A somewhat similar law was previously passed in Louisiana and similar bills have been urged or introduced in a number of other states.[4]

A. Linking Software Piracy Abroad to Unfair Competition and Job Loss in Washington

Software piracy is a major issue facing businesses in Washington State according to the Act's proponents.[5] This problem is most notable in Asia and Latin America.[6] For example,

---

House concurred to amended bill and passed new version of Sub. H.B. 1495 by a vote of 85-11 on April 5, 2011. Washington State Governor Chris Gregoire signed the Act into law on April 18, 2011. *See* FINAL SUB. H.B. REP. 62-1495, Reg. Sess. (Wash. 2011); *see also* Sharon Pian Chan, *State Passes Anti-Piracy Law to Help Microsoft*, SEA. TIMES, Apr. 5, 2011, http://seattletimes.nwsource.com/html/microsoft/2014693401_microsoft06.html [hereinafter Pian Chan, *State Passes Anti-Piracy Law*].

[3] WASH. REV. CODE § 19.330.090 (2011).

[4] See LA. REV. STATE ANN. § 51:1427 (2011); S.B. 1529, 50th Leg., 1st Reg. Sess. (Ariz. 2011); A.B. 473, 2011 Assemb., Reg. Sess. (Cal. 2011); H.B. 6619, 2011 Gen. Assemb., Jan. Sess. (Conn. 2011); S.B. 529, 117th Gen. Assemb., 1st Reg. Sess. (Ind. 2011); H.R. 113, 2011 Gen. Assemb., Reg. Sess. (Ky. 2011); H.B. 2842, 187th Gen. Ct. (Mass. 2011); H.B. 1022, 96th Gen. Assemb., 1st Reg. Sess. (Mo. 2011); A.B. 3915, 2011 Assemb., 234th Legis. Sess. (N.Y. 2011); H.B. 672, 2011 Gen. Assemb., Reg. Sess. (N.C. 2011); OR H.B. 3315, 76th Legis. Assemb., 2011 Sess. (Or. 2011); S.B. 201, 59th Leg., Gen. Sess. (Utah 2011).

[5] According to State Representative Deb Eddy, a Democrat from Kirkland and original sponsor of S.H.B. 1495, "[w]e have a problem internationally with stolen and counterfeited software." Sharon Pian Chan, *Microsoft Presses State to Tackle Software Piracy*, SEA. TIMES, Mar. 12, 2011, http://seattletimes.nwsource.com/html/businesstechnology/2014472018_btpiracy14.html [hereinafter Pian Chan, *Microsoft Presses State*].

[6] During public testimony before the Senate Labor, Commerce & Consumer Protection Committee, Nancy Anderson, Microsoft Corporate Vice President and Deputy General Counsel, Legal and Corporate Affairs, identified piracy in Asia and Latin America as an "intractable problem" for the technology industry in Washington. *Senate Labor, Commerce & Consumer Protection Cmte., March 14, 2011*, TVW (Nov. 5, 2011) http://www.tvw.org/media/mediaplayer.cfm?evid=2011030108&TYPE=V&CFID=8409116&CFTOKEN=46667469&bhcp=1, at 16:50.

in China, 86 percent of PC users acquire their software illegally most or all of the time.[7] The piracy statistics are similar in developing countries across Asia, Africa, and Latin America.[8]

Enforcement of IP rights overseas may be challenging. Given current conditions, lax IP protections abroad result in limited legal remedies for IT license holders in the United States.[9] By allowing technology companies to enforce ownership rights in Washington, advocates claimed, the Act would "give the tech industry the ability to keep growing and keep adding jobs."[10] In addition, the Act ensures fairness among competing manufacturers by eliminating the economic advantage gained through unlawful use of IT.[11]

B. Controversy and Criticism of the Act

Various companies and associations voiced opposition to the Act.[12] Opponents raised several issues both in public testimony

---

[7] Business Software Alliance, BSA GLOBAL SURVEY OF PC USER ATTITUDES, 2010–11, 2, http://portal.bsa.org/globalpiracy2010/downloads/opinionsurvey/survey_global.pdf.

[8] *Id.*

[9] Explained Brad Smith, Microsoft General Counsel and Executive Vice President, Legal and Corporate Affairs, "[Companies in other countries] tell us they have no intention of paying for something they can steal with immunity." Pian Chan, *Microsoft Presses State*, *supra* note 5.

[10] *Senate Labor, Commerce & Consumer Protection Cmte., March 14, 2011*, TVW (Nov. 5, 2011), http://www.tvw.org/media/mediaplayer.cfm?evid=2011030108&TYPE=V&CFID=8409116&CFTOKEN=46667469&bhcp=1, at 16:40; Pian Chan, *Microsoft Presses State*, *supra* note 5.

[11] Unfair competition law is generally considered a doctrine of intellectual property law, originally focused on preventing one party from passing off his goods or business as the goods or business of another. 74 AM. JUR. 2D TRADEMARKS AND TRADENAMES § 82 (2011 ed.). The law has increased in scope with the passage of federal and state consumer protection laws, which are broadly construed to protect both consumers and other businesses from unfair business practices. 17 AM. JUR. 2D CONSUMER PROTECTION § 268 (2011 ed.). However, the Act is not part of the Washington Consumer Protection Act and represents a new expansion of unfair competition law in Washington. WASH. REV. CODE § 19.330.100 (2011).

[12] Those sharing concerns included IBM, Hewlett-Packard, Dell, Intel, Motorola, Fred Meyer, the Software & Information Industry Association, the

and during floor debate.[13] First, opponents pointed to what they perceived as broad and ambiguous language.[14] Detractors argued that the Act was hard to understand and that the language used creates business uncertainty, which hurts American businesses.

Opponents also pointed to increased costs associated with the new requirements placed on third-party businesses to "police" their suppliers.[15] Retailers argued that the law will force them to further

---

Washington Retail Association, and the Washington Newspaper Publishers Association.

[13] For example, during floor debate prior to passage of the amended bill in the Senate, Republican Senator Jim Honeyford, Sunnyside, attempted to subvert the bill by introducing an amendment that would have required additional research, rather than create a new cause of action. Senator Honeyford raised familiar objections to the bill, including that the bill was overbroad, would require affirmative actions on the part of retailers, and would not work as intended. The Senator also noted the opposition in the business community. However, the amendment failed. *Senate Floor Debate, Segment: B, April 4, 2011*, TVW (Oct. 23, 2011), http://www.tvw.org/media/mediaplayer.cfm?evid=2011040041B&TYPE=V&CFID=8409116&CFTOKEN=46667469&bhcp=1, at 1:05:11.

[14] Ken Wasch, president of the Software & Information Industry Association, wrote, "[W]e are very concerned that several of the provisions in the bill in conjunction with broad or undefined language used in the bill could lead to unintended consequences that will produce opportunities for harassment of legitimate businesses and fuel more business uncertainty." Letter from Ken Wasch, President, Software & Information Industry Association, to Jamie Pedersen, Chairman, House Judiciary Committee, Washington State House of Representatives (Feb. 2, 2011) [hereinafter Letter from Ken Wasch].

[15] According to Jan Teague, President and CEO, Washington Retail Association, "[the Act] would require large companies to establish expensive tracking to ensure their suppliers were not using illegal software." Teague went on to compare the issues faced by Microsoft and other technology companies to those faced by retailers:

> [P]iracy is Microsoft's problem to solve as it has been trying to do for several years. It is a problem akin to what retailers call "shrink," or the loss of income from merchandise stolen either by outsiders or employees. Unfortunately, shrink is a painful cost of doing business. But retailers no more would seek Microsoft's help with this problem than Microsoft should be asking retailers to help pay for solving its challenges with software piracy.

Jan Teague, Guest Column, *Microsoft Software-Piracy Bills would Harm Businesses*, SEATTLEPI.COM, Mar. 11, 2011, http://blog.seattlepi.com/microsoft/2011/03/11/guest-column-microsoft-software-piracy-bills-would-harm-

vet computers and electronics coming from abroad, adding costs to already expensive supply chains.[16]

Finally, opponents contended that the Act exposes them to threats of frivolous litigation and discovery abuses.[17] Detractors noted that the possibility of litigation and discovery, even if limited by court approval and discovery rules, could be abused by "unscrupulous businesses" seeking to gain a competitive advantage through abuse of the new cause of action.[18]

C. Similar Bills and Legislation

The Washington statute represents a new approach to combating unfair practices by manufacturers. Only one state, Louisiana, has passed a remotely similar law, codified as La. Rev. Stat. § 51:1427 (2011). However, the Louisiana law is incorporated into that state's unfair trade and consumer protection law, rather than functioning as a separate cause of action. The statute covers both the development and manufacture of a product as well as the development and provision of services using stolen or misappropriated property, making it more expansive than the Washington Act. To date, no reported decisions have addressed claims under the Louisiana law. At the urging of Microsoft, bills similar to S.H.B. 1495 were introduced but not passed in a number of other states in 2011, including Arizona, California, Connecticut,

---

businesses.

[16] Valdes, *supra* note 1.

[17] According to a letter from eighteen technology companies, including IBM, Dell, Intel and Motorola:

> American businesses that unwittingly buy from companies alleged to be using unlicensed software could be unfairly penalized. The onerous remedies in the bill — including monetary damages, potential seizure of products, and injunctions barring sale of products in the state — would invite baseless and burdensome litigation that could be used in an anti-competitive manner.

Letter from technology companies to Jamie Pedersen, Chairman, House Judiciary Committee, Washington State House of Representatives (Mar. 11, 2011); Valdes, *supra* note 1.

[18] Letter from Ken Wasch, *supra* note 13.

Indiana, Kentucky, Massachusetts, Missouri, New York, North Carolina, Oregon, and Utah.[19]

II. A NEW CAUSE OF ACTION

Wash. Rev. Code § 19.330.020 creates a new cause of action for both the Washington attorney general and private plaintiffs. A person is "deemed to engage in an unfair act where [an article or product manufactured while using stolen IT] is sold or offered for sale in this state, either separately or as a component of another article or product."[20] Two types of parties face possible liability under the new cause of action: manufacturers and third-party businesses.

A. Possible Defendants

Manufacturers are the primary targets of the new cause of action.[21] To be liable, a manufacturer must (1) produce a tangible article or product while (2) using stolen IT in its business operations. The Act excludes from its definition of "article or product" all services, including restaurant services; products subject to regulation by the Federal Food and Drug Administration (FDA) that are primarily used for medical or medicinal purposes; and food and beverages.[22]

---

[19] *See* S.B. 1529, 50th Leg., 1st Reg. Sess. (Ariz. 2011); A.B. 473, 2011 Assemb., Reg. Sess. (Cal. 2011); H.B. 6619, 2011 Gen. Assemb., Jan. Sess. (Conn. 2011); S.B. 529, 117th Gen. Assemb., 1st Reg. Sess. (Ind. 2011); H.R. 113, 2011 Gen. Assemb., Reg. Sess. (Ky. 2011); H.B. 2842, 187th Gen. Ct. (Mass. 2011); H.B. 1022, 96th Gen. Assemb., 1st Reg. Sess. (Mo. 2011); A.B. 3915, 2011 Assemb., 234th Legis. Sess. (N.Y. 2011); H.B. 672, 2011 Gen. Assemb., Reg. Sess. (N.C. 2011); OR H.B. 3315, 76th Legis. Assemb., 2011 Sess. (Or. 2011); S.B. 201, 59th Leg., Gen. Sess. (Utah 2011). The Utah bill failed after it received strong opposition from the Utah Food Industry Association and Utah Retail Merchants Association.[19]*2011 Legislative Wrap-Up*, Utah Food Industry Association / Utah Retail Merchants Association, http://www.utfood.com/UFIA/PDF_files/2011%20Legislative%20Wrap%20Up.pdf.

[20] WASH. REV. CODE § 19.330.020 (2011).

[21] *See id*.

[22] *Id.* at § 19.330.010(1)(a).

For the purposes of the Act, "IT" is defined broadly as proprietary hardware or software technology that can be owned or licensed.[23] However, the IT must be available for retail purchase on a stand-alone basis at or before the time it was acquired, appropriated, or used.[24] As a result, the Act does not function to protect a company's proprietary trade secrets.[25]

As defined by the Act, "business operations" include the manufacture, distribution, marketing, or sales of a product or article.[26] For example, use of pirated software in back-office accounting processes would create liability under the Act so long as the accounting processes relate to a product or article sold or offered for sale in Washington.

The Act also allows for a secondary claim for actual direct damages against a third party that "sells or offer[s] to sell in [Washington] state products made by [a manufacturer] in violation of section 2 of [the Act]."[27]

B. Possible Plaintiffs

Either the Washington attorney general or a private plaintiff may utilize the new cause of action.[28] To qualify as a private plaintiff, a party must be a manufacturer with products sold or offered for sale in Washington that are in direct competition with the products of a manufacturer accused of violating the Act.[29] The

---

[23] *Id.* at § 19.330.010(7)(a).

[24] *Id.* at § 19.330.010(7)(a).

[25] The Act deals specifically with stolen IT, rather than IP more generally. Whereas IP consists of "intangible rights protecting commercially valuable products of the human intellect," which can include trademarks, copyrights, patents, trade secrets, publicity rights, moral rights, and rights against unfair competition, BLACKS LAW DICTIONARY 368 (3d Pocket ed. 2006); WASH. REV. CODE § 19.330.010(7)(a) (2011), the IT defined in the Act is limited to hardware or software, which are the manifestations of concepts generally protected by IP law.

[26] WASH. REV. CODE § 19.330.010(7)(b) (2011).

[27] *Id.* at § 19.330.060(2).

[28] *Id.* at §§ 19.330.060(1), 19.330.060(5).

[29] *Id.* at § 19.330.060(5); *see* § IV(B), *infra*.

Washington attorney general may proceed on behalf of any qualifying manufacturer.[30]

III. JURISDICTION

The Act provides for jurisdiction based on both personal and quasi *in rem* jurisdiction theories. Most manufacturers will fall within the personal jurisdiction of Washington courts based on Washington's long-arm statute.[31] However, a Washington court may not have personal jurisdiction over a manufacturer that has never visited the state and has no assets within the state. In such a case, the Act authorizes a Washington court to proceed *in rem*, entering judgment against property owned by the manufacturer that is located in the state, such as products stored there.[32]

A. Personal Jurisdiction

The primary method for obtaining jurisdiction under the Act is by establishing personal jurisdiction under Washington's long-arm statute, Wash. Rev. Code § 4.28.185(1)(a) (2011). Section 2 of the Act invokes the long-arm statute, which allows for personal jurisdiction over any person, including a foreign corporation, who transacts business in the state.[33] Most manufacturers offering a product or article for sale in Washington or delivering a product or article that is a component of an end product offered for sale in Washington will fall within the extensive personal jurisdiction provided by Wash. Rev. Code § 4.28.185 1(a) (2011).[34]

B. Quasi In Rem *Jurisdiction*

When a court cannot exercise personal jurisdiction, the Act allows a plaintiff to seek recovery by subjecting the defendant

---

[30] *Id.* at § 19.330.060(1).

[31] *See id.* at § 4.28.185(1)(a).

[32] *Id.* at § 19.330.070(1).

[33] *Id.* at § 4.28.185(1)(a) (2011); 14 KARL B. TEGLAND, WASHINGTON PRACTICE SERIES, CIVIL PROCEDURE § 4.7 (2011 ed.).

[34] *See, e.g.*, TEGLAND, *supra* note 34, at § 4.7.

manufacturer's property to the discharge of the plaintiff's claims. The Act provides Washington courts with jurisdiction to "proceed *in rem* against any articles or products" located in Washington that are the subject of the action and to which the defendant still holds title.[35] Although the law refers to this type of action as *in rem*, it is actually a *quasi in rem* proceeding.[36]

Attachment of property located in Washington may occur any time at or after the filing of the complaint, "regardless of the availability or amount of any monetary judgment."[37] It is important to note that this type of jurisdiction is limited to property to which the alleged violator still holds title.[38] For example, a manufacturer's products that have already been sold to a wholesaler would not be subject to attachment.

IV. PROCEEDING WITH A CLAIM

For a plaintiff to proceed with a claim under the Act, the IT owner must provide specific notice to the alleged violator and meet a burden of proof for the notice. The plaintiff also must meet certain standing requirements. A plaintiff meeting these requirements can potentially seek both injunctive relief and money damages against a manufacturer. In certain circumstances, a plaintiff may also seek actual direct damages against a third party.

A. Notice

Specific notice is required by the Act. For a plaintiff to proceed under the new cause of action, the IT owner or exclusive licensee, or the owner's agent, must provide 90-days' notice to the alleged violator.[39] Under penalty of perjury, the notice must: (1) identify

---

[35] WASH. REV. CODE § 19.330.070(1).

[36] Whereas *in rem* proceedings "involve an adjudication as to the status of, or interests in, or title to, property," *quasi in rem* proceedings allow a court to "assert jurisdiction over a nonresident defendant because the defendant owns property in Washington." TEGLAND, *supra* note 34, at § 4.7.

[37] WASH. REV. CODE § 19.330.070(1).

[38] *Id.* at § 19.330.040.

[39] *Id.* at § 19.330.050(1).

the stolen or misappropriated IT; (2) identify the lawful owner of the IT; (3) identify the local law allegedly violated and state that the notifying party has a reasonable belief that the party being notified has acquired, appropriated, or used the IT unlawfully; (4) state how the IT is being used by the party being notified, if known by the notifying party; (5) state the manufactured articles or products to which the IT relates; and (6) specify the basis and evidence for the allegation.[40] If, upon receiving notice, an alleged violator "proceeds diligently" to replace its unlawful IT with legal IT, the notice period must be increased by an additional 90 days, allowing for 180 days to comply.[41] The rightful owner of the IT may also voluntarily extend the period for compliance.[42]

In addition to providing specific information in the 90-day notice, the notifying party must perform a "reasonable and good faith investigation" verifying that the information in the notice provided to the alleged violator is "accurate based on the notifier's reasonable knowledge, information, and belief."[43] This represents a relatively low burden of proof for notice, given the means by which technology companies such as Microsoft can track piracy.[44] Microsoft appears confident that it and other companies in the technology industry can meet the requirements of this notice standard.[45]

---

[40] *Id.* at § 19.330.050(2).

[41] *Id.* at § 19.330.050(1).

[42] *Id.*

[43] *Id.* at § 19.330.050(3).

[44] *See, e.g.*, Michael Kan, *Software Tracking Could Turn Chinese Piracy into Revenue*, INFOWORLD.COM, Aug. 29, 2011, http://www.infoworld.com/d/the-industry-standard/software-tracking-could-turn-chinese-piracy-revenue-171036?page=0,0; Mark Hachman, *CSI Redmond: How Microsoft Tracks Down Pirates*, PCMAG.COM, Apr. 26, 2010, http://www.pcmag.com/article2/0,2817,2363041,00.asp.

[45] *See Senate Labor, Commerce & Consumer Protection Cmte., March 14, 2011*, TVW (Nov. 5, 2011), http://www.tvw.org/media/mediaplayer.cfm?evid=2011030108&TYPE=V&CFID=8409116&CFTOKEN=46667469&bhcp=1, at 20:30.

B. Standing

To have standing to seek damages under the Act, a party must prove three elements by a preponderance of the evidence. The party must prove that: (1) it manufactures products sold or offered for sale in Washington in competition with articles or products made using stolen IT; (2) it does not use stolen IT to make its products; and (3) it suffered economic harm, which may be evinced by showing that the retail price of the stolen IT was at least $20,000.[46] To proceed *in rem* or to seek injunctive relief, a party must also demonstrate that it suffered "material competitive injury" as a result of the violation.[47] To show a material competitive injury, a plaintiff must demonstrate that over a four-month period there was "at least a three percent retail price difference" between a product made by a violator and a competing product made by the plaintiff.[48] This provision has the effect of limiting any injunctive or *in rem* relief to a subset of plaintiffs that can prove significant competitive harm over an extended period.

C. Remedies Available

If an alleged violator continues to use stolen IT after receiving 90 days' notice, the plaintiff, after establishing standing, may seek both injunctive relief and money damages. A court may also enjoin the sale of products in Washington when a defendant lacks sufficient attachable assets to satisfy a judgment. In addition, the Act allows a plaintiff seek actual direct damages against a third party in certain circumstances.

1. Injunctive Relief

The Act provides for injunctive relief both before and after judgment. After the 90-day notice period has expired and an alleged violator has not taken any affirmative action to cure the violation, a court may enjoin the violator from selling or offering

---

[46] WASH. REV. CODE §§ 19.330.060(5)(a–c).
[47] *Id.* at § 19.330.060(5)(d).
[48] *Id.* at § 19.330.010(5).

to sell goods made with stolen IT in Washington.[49] A court may enforce the injunctive relief prior to any determination that a violation of the Act occurred.

There are several limitations on the use of injunctive relief. An injunction is not available against products "to be provided" to a third party that has satisfied an affirmative defense under one of the Act's safe harbor provisions.[50] Injunctive relief is also not available against products that are an "essential component" of a third party's product or article, meaning that: (1) the third party receives the product pursuant to a contract or purchase order; (2) the third-party product will not perform as intended without the product; and (3) no substitute product is available that offers the similar functionalities with similar quality and a comparable price.[51]

If, after a court determines that a violation of the Act has occurred, the violator lacks sufficient attachable assets in Washington to satisfy a judgment against it, a court may enjoin the sale or offering for sale in Washington of any products manufactured in violation of the Act.[52] However, a court may not enjoin the sale of any such products by parties other than the manufacturer.[53]

2. Money Damages

Money damages are also available to plaintiffs. A plaintiff may seek from the violating manufacturer the greater of actual damages or three times the retail price of the stolen IT.[54] For purposes of damages, retail price is determined by multiplying the cost of the stolen technology by the number of stolen items used.[55] Thus, if a manufacturer is using 1,000 pirated copies of the Microsoft Office Professional software, and Microsoft Office Professional software

---

[49] *Id.* at § 19.330.060(1)(a).
[50] *Id.; see* § V, *infra*.
[51] *Id.* at § 19.330.060(6)(b); *id.* at § 19.330.010(3).
[52] *Id.* at § 19.330.060(6)(a).
[53] *Id.* at § 19.330.040.
[54] *Id.* at § 19.330.060(1)(b).
[55] *Id.* at § 19.330.010(6).

costs $500 per license, the retail price is $500,000. The Act offers no instruction as to how "actual damages" are determined. It is unclear if damages may or must stem from the harm done to the competing manufacturer, from the illegal use of IT, or both.[56] In any case, treble damages may be awarded when a court finds that the use of the stolen IT is "willful."[57]

3. Actual Direct Damages Against a Third Party

If and only if a court has entered judgment against a violating manufacturer, a plaintiff may add to the action a claim for actual damages against a third party who sells the products made with the stolen IT.[58] However, a third-party business that sells products manufactured by the violating manufacturer is liable only under certain circumstances.

a. Conditions Required for Action Against a Third Party

A third-party business is liable for actual direct damages under the Act only if five conditions are met.

First, the third-party business must receive written notice of the claim at least 90 days prior to entry of the judgment against the manufacturer.[59] This means that to preserve the possibility of a third-party claim, in addition to notifying an alleged violating manufacturer, a plaintiff IT owner or exclusive licensee must also provide notice to any third-party business that sells the manufacturer's products.

Second, the violating manufacturer must fail to make an appearance or must lack sufficient attachable assets to satisfy a judgment against it.[60] If the violating manufacturer appears or

---

[56] For example, it is unclear whether "actual damages" should be computed based on loss of sales, differences in production or marketing costs attributed to the use of stolen IT, or some other form of economic harm.

[57] WASH. REV. CODE § 19.330.060(4)(a).

[58] *Id.* at § 19.330.060(2).

[59] *Id.* at § 19.330.060(2)(a).

[60] *Id.* at § 19.330.060(2)(b).

satisfies the judgment against it, a plaintiff may not proceed against a third-party business.

Third, the violating manufacturer must make the end product sold by the third-party business or make a component worth 30 percent or more of the total value of the third-party business' end product.[61] Thus, a third-party business will not be held liable for purchasing minor components used to create an end product sold or offered for sale in Washington.

Fourth, the third-party business must have a direct contractual relationship with the violating manufacturer.[62] If, for example, the third-party business has a contractual relationship with a reseller, rather than the manufacturer, the third-party business cannot be added to the claim.

Finally, the third-party business must not have adjudicated the matter or be in the process of adjudicating the matter in any other state or federal court.[63] A prior final judgment or settlement or any ongoing litigation arising out of the same theft of IT precludes action in Washington.

b. Possible Damages Recoverable Against a Third Party

If all five conditions are met, a plaintiff may seek actual direct damages against the third-party business, so long as the third-party business has not availed itself of any of the safe harbor provisions included in the Act.[64] Damages against a third-party business must be the lesser of the retail price of the stolen IT (the cost of the stolen technology multiplied by the number of stolen items used) or $250,000.[65]

V. PROTECTIONS AND SAFE HARBOR PROVISIONS

Though the Act subjects both manufacturers and third-party businesses doing business in Washington to potential liability, it

---

[61] *Id.* at § 19.330.060(2)(c).
[62] *Id.* at § 19.330.060(2)(d).
[63] *Id.* at § 19.330.060(2)(e).
[64] *See* Section V, *infra*.
[65] WASH. REV. CODE § 19.330.060(3).

also includes a number of safe harbor provisions and procedural safeguards. By taking advantage of these provisions, both manufacturers and third-party businesses can limit their exposure to liability.

A. Exemptions for Manufacturers

Both manufacturers and third parties can avoid suit in Washington if they have already adjudicated the matter or are in the process of adjudicating the matter in any other state or federal court.[66] In addition, the Act contains several explicit exemptions for manufacturers.

First, a manufacturer is not liable under the Act if it manufactures an end product that is copyrightable.[67] Specifically, the Act exempts end products that fall under United States copyright law.[68] As a result, this exception protects manufacturers who work for companies that produce copyrighted software.[69]

Second, products that are manufactured by or for a copyright owner and display copyrighted work or materials related to theme parks are exempted.[70] This exception was most likely added at the behest of the Motion Picture Association of America, which expressed concerns during the initial drafting process.[71]

Third, the Act exempts products that are packaging for a copyrightable product or material related to theme parks.[72] This exemption essentially expands the first two exemptions, protecting not only copyrightable products and theme park promotional goods, but also the packaging for those products.

Fourth, the Act does not apply where the allegation is based on

---

[66] *Id.* at §§ 19.330.060(1)(c), 19.330.060(2)(e).

[67] *Id.* at § 19.330.030(1)(a).

[68] *Id.* at § 19.330.010(2).

[69] Thus, Microsoft Corp. would not face litigation if it contracted with a manufacturer in China to produce software and that manufacturer used pirated software in its back-office operations.

[70] WASH. REV. CODE § 19.330.030(1)(b).

[71] *House Judiciary Committee, February 2, 2011*, TVW (Nov. 7, 2011), http://www.tvw.org/media/mediaplayer.cfm?evid=2011021026&TYPE=V&CFID=8409116&CFTOKEN=46667469&bhcp=1, at 1:32:20.

[72] WASH. REV. CODE § 19.330.030(1)(c).

patent infringement or trade secret misappropriation.[73] Instead, such claims should be prosecuted under Title 35 of the United States Code.[74] This exemption avoids conflicts with federal law by limiting the ability of patent holders to use the Act to prosecute patent violations.

Fifth, the Act does not allow an allegation based on "a claim that the defendant's use of the IT violates the terms of a license that allows users to modify and redistribute any source code associated with the technology free of charge."[75] Thus, a claim based on the use of so-called "open source" software is prohibited. Even if, for example, a manufacturer is using a specially licensed version of Linux operating system in violation of that license, a plaintiff probably would not have a claim because the underlying Linux source code can be modified and redistributed free of charge.[76]

Finally, the allegation may not be based on providing an additional party with access to stolen IT, rather than using the IT in business operations.[77] This exemption limits the scope of the Act to only those manufacturers that are actually using stolen IT. If an IT owner or exclusive licensee is claiming that the defendant merely acted as an intermediary by providing some other party with the stolen IT, it must use other legal avenues to pursue that claim.

B. Protections for Third Parties

The Act contains a number of safe harbors that can be invoked by a third-party business after the business receives notice. Three of these safe harbor provisions are simple to invoke, whereas three additional provisions require more complex actions on the part of

---

[73] *Id.* at § 19.330.030(2).

[74] *Id.*

[75] *Id.* at § 19.330.030(3).

[76] Pamela Jones, *Why Is Microsoft Seeking New State Laws That Allow it to Sue Competitors For Piracy by Overseas Suppliers?*, GROKLAW (Nov. 27, 2011, 12:45 PM), http://www.groklaw.net/articlebasic.php?story=2011032316585825.

[77] WASH. REV. CODE § 19.330.030(4).

the third-party business. In each case, the third-party business must be given an opportunity to plead an affirmative defense based on one or more of the safe harbor provisions after it has received proper notice.[78]

1. Simple Safe Harbor Provisions

A third-party business may avoid liability by proving by a preponderance of the evidence the existence of one of three factual scenarios. First, the third-party business may prove that it is an end consumer or end user of the product being manufactured.[79] Second, the third-party business may prove that it has annual revenues of $50 million or less.[80] Third, the third-party business may prove that it does not have a contractual relationship with the violating manufacturer.[81]

2. Complex Safe Harbor Provisions

A third-party business may also avoid liability by proving by a preponderance of the evidence one of three complex affirmative defenses. Each safe harbor provision involves several steps.

a. Prior Agreement

First, a third-party business may avoid liability by proving (1) that it acquired the products under an agreement entered into prior to January 18, 2012, and (2) that within 180 days of receiving notice of the manufacturer's violation, the third-party business either requested and received written proof of compliance or sent a letter demanding compliance and proof of compliance.[82] If the violating manufacturer does not cure the violation and the third-party business does not take action within 180 days, the third-party

[78] *Id.* at § 19.330.080(1).
[79] *Id.* at § 19.330.080(1)(a).
[80] *Id.* at § 19.330.080(1)(b).
[81] *Id.* at § 19.330.080(1)(e).
[82] *Id.* at § 19.330.080(1)(c)(ii).

business may instead cease business with the violator as is feasible under the terms of the contract.[83]

b. Good-Faith Reliance or Written Assurances

A third-party business may avoid liability by proving either, (1) that it acquired the products with good faith reliance on a code of conduct or contract requiring compliance with applicable law, or that it received written assurances of compliance from the manufacturer, and (2) within 180 days of receiving notice of the violation, the third-party business either requested and received written proof of compliance, or sent a letter demanding compliance and proof of compliance.[84] If the violating manufacturer does not cure the violation and the third-party business does not take action within 180 days, the third-party business may alternatively cease business with the violator as is feasible under the terms of the contract.[85]

c. Commercially Reasonable Efforts

A third-party business may avoid liability by proving that it made "commercially reasonable efforts to implement practices and procedures" requiring its manufacturers not to use stolen IT. Such efforts can be proven by presenting evidence that the third-party business implemented a code of conduct that prohibits use of stolen IT. The code of conduct must include requirements that the manufacturer submit to audits of their IT practices and state that the third-party business either has a practice of auditing "in accordance with generally accepted industry standards" or engages a third party association to perform auditing. The code must also state that a violation of the Act constitutes a breach of contract. Alternatively, the third-party business may avoid liability by proving it adopted and undertook "commercially reasonable efforts" to implement a code of conduct, and undertook practices

---

[83] *Id*.
[84] *Id.* at § 19.330.080(1)(c)(i).
[85] *Id.* at § 19.330.080(1)(c)(ii)(C).

and procedures to ensure compliance with the Act.[86]

3. Procedural Safeguards

The Act includes several safeguards for third-party businesses impacted by *in rem* actions, as well as protections against discovery abuse. *In rem* actions may not proceed against products to which title has transferred from the manufacturer to the third party.[87] As a result, once title transfers from the manufacturer to the third-party business, the third-party business need no longer be concerned about attachment. In addition, a court must notify any third-party business in possession of products subject to an *in rem* proceeding 90 days in advance of the pending attachment order.[88] Once this notice is provided, a third party may avoid the attachment order by establishing that the third party has an affirmative defense under a safe harbor provision or by posting a bond with the court of up to $25,000.[89]

Discovery is only allowed against a third-party business after all discovery between the plaintiff and manufacturer is complete and only if the evidence produced through that discovery does not resolve an issue of material dispute.[90] Thus, the Act limits discovery against third-party businesses to specific information related to a material dispute between the plaintiff and the defendant. Furthermore, if such discovery involves confidential or sensitive information, that information is subject to a protective order.[91] As a result, the Act protects third-party businesses from broad and invasive discovery requests.

VI. PRACTICAL STEPS FOR THIRD-PARTY COMPLIANCE

In addition to relying on one of the safe harbors provisions, a third-party business concerned about possible liability may take

---

[86] *Id.* at § 19.330.080(1)(d).
[87] *Id.* at § 19.330.070(1).
[88] *Id.* at § 19.330.070(2).
[89] *Id.*
[90] *Id.* at § 19.330.080(4).
[91] *Id.* at § 19.330.080(5).

two concrete steps to help avoid litigation. First, the business should create or update a code of conduct for manufacturers that it includes in all contractual relationships. Second, if it is financially feasible, the business should integrate checks on IT use into existing supply-chain management practices. The business also should also make use of demand letters, as described in the Act.

A. Code of Conduct and Supply Chain Management

A business should institute or update a code of conduct applicable to contracted manufacturers that requires compliance with all applicable laws prohibiting the use of stolen IT by the manufacturer. By doing so, a business positions itself to take advantage of the safe harbor provisions of the Act while also putting manufacturers on notice of its expectations regarding IT piracy.

The business should also integrate checks on IT use into existing supply-chain management practices to effectively "scrub" the supply chain for stolen IT. A business with existing supply-chain management capabilities should consider contractually requiring submission to audits and instituting additional auditing processes similar to those used to ensure compliance with labor or Securities and Exchange Commission reporting requirements.[92] Depending on the level of sophistication of the company and the type of industry, this type of oversight may be more cost-effectively handled by a third-party service provider. Creating an auditing process to ensure compliance throughout the supply chain will best ensure that a business completely avoids litigation under the Act.

B. Demand Letter

In some cases, it may be more practical for a third-party business to rely on sending demand letters as required by the Act, rather than implementing auditing processes or engaging a third

---

[92] *See, e.g.*, DODD-FRANK WALL STREET REFORM AND CONSUMER PROTECTION ACT, Pub. L. No. 111-203, § 1502, 124 Stat. 2213.

party to perform auditing. However, it is unclear what impact a demand letter would have on a contractual relationship. Under U.C.C. § 2-609, failure to provide adequate assurance of performance is grounds to breach a contract.[93] Given the language in the Act, it appears that a company could send a demand letter and then continue its contractual relationship with the offending manufacturer, at least until a suitable replacement manufacturer in compliance can be found.

VII. PREEMPTION ISSUES

During the debate preceding passage of the Act, opponents raised the possibility that federal law may preempt or preclude the state law.[94] There are at least two possible ways that such an argument might proceed: (1) intrusion into the federal power to regulate foreign commerce or (2) preemption due to conflict with Federal Copyright statutes.[95] Notably, the Act contains a severability clause.[96]

The (Foreign) Commerce Clause argument is premised on the Act's potential conflict with federal trade agreements or treaties or federal international commerce policy generally. A party arguing such a theory would need to demonstrate a sufficiently clear conflict between a federal foreign policy and the Act. The party would support its argument by pointing to evidence of federal intent in conflict with the intent or effect of the Act.[97] The fact that the state law targets foreign corporations rather than foreign governments should not be determinative.[98] Any potential argument would need to be evaluated on a country-by-country

---

[93] U.C.C. § 2-609(4) (2003).

[94] Jan Teague, Guest Column, *Microsoft Software-Piracy Bills would Harm Businesses*, SEATTLEPI.COM, Mar. 11, 2011, http://blog.seattlepi.com/microsoft/2011/03/11/guest-column-microsoft-software-piracy-bills-would-harm-businesses.

[95] *See generally*, U.S. CONST. art. I, § 8, cl. 3; 17 U.S.C. (2010).

[96] Ch. 98, § 11, 2011 Wash. Sess. Laws 882.

[97] American Insurance Association v. Garamendi, 539 U.S. 396 (2003); Zschernig v. Miller, 389 U.S. 429 (1968); U.S. CONST. art. I § 8 cl. 3.

[98] *Garamendi*, 539 U.S. at 415–16.

basis, taking into account any evidence of federal intent regarding foreign manufacturing.

By comparison, a theory of preemption based on the Act's conflict with federal copyright statutes is premised on the claim that the Act invades federal law under the auspices of unfair trade law. Claim preemption "occurs frequently in cases involving copyright preemption of state claims and, often, turns on an effort by a litigant to bend existing state law to fit a remedy that more properly would be available under copyright law."[99]

The Act's drafters included language that appears to be designed to avoid this form of preemption. The language in the Act repeatedly links the cause of action to the harm to competition and specifically limits the class of plaintiffs to competing manufacturers.[100] The Act does not create an explicit competing cause of action, nor does it allow for a claim if action is taken under federal copyright law.[101]

Despite careful attention to drafting, the Act still raises potential claim preemption issues. Federal copyright law dictates that all "legal or equitable rights that are equivalent to any of the exclusive rights within the general scope of copyright . . . in works of authorship that are fixed in a tangible medium of expression and come within the subject matter of copyright . . . are governed exclusively by [the Copyright Act]."[102] Federal law has preempted claims for recovery of damages based on contract breach.[103] Claims under the Act, although based on unfair competition allegations, may be interpreted as intruding on an area occupied by federal copyright law because of the apparent overlap between the definition of IT in the Act and the traditional scope of copyright law.

---

[99] Raymond T. Nimmer, *Federal Preemption in Intellectual Property Law*, in PATENTS, COPYRIGHTS, TRADEMARKS, AND LITERARY PROPERTY COURSE HANDBOOK SERIES 95, 102 (1996).

[100] *See* WASH. REV. CODE §§ 19.330.010(5), 19.330.020, 19.330.060(5) (2011).

[101] WASH. REV. CODE §§ 19.330.060(1)(c), 19.330.060(2)(e) (2011).

[102] 17 U.S.C. § 301(a) (2010).

[103] Benjamin Capital Investors v. Cossey, 126 Or. App. 135, 867 P.2d 1388 (1994).

CONCLUSION

Piracy is a problem for IT owners and exclusive licensees, as well as for American businesses. The Act attempts to provide recourse for technology companies and manufacturers doing business in Washington. It is possible that faced with pressure from both IT owners and their U.S-based business partners, foreign manufacturers will begin to bring their IT into compliance. It is also possible that some manufacturers will find alternatives to avoid prosecution, such as creating separate reselling companies to sell into the Washington market.

Regardless of how foreign manufacturers respond, given the safe harbor provisions and procedural safeguards included in the Act, educated and aware third-party businesses can avoid liability by taking relatively simple steps. In particular, businesses with existing complex supply-chain management systems should be able to adjust quickly to the new requirements of the Act by integrating a tracing mechanism into the systems. However, even the smallest company can protect itself by taking the basic step of sending a demand letter once it receives notice of an alleged violation.

Using unfair competition law to address problems of piracy and infringement is a novel and unproven approach; it remains to be seen how companies will use the Act (if at all), as well as how effective the Act will prove in changing the behavior of manufacturers and their third-party business partners. It may be that no party is particularly interested in litigation. As written, the Act seems more effective in promoting changes within the business community by inviting industry changes to codes of conduct and supply chain management.

Regardless of whether the Act prevents IT piracy and unfair competition, the law may still serve the interests of Microsoft and other IT owners. Should the Act prove effective, proponents can use it as a model for other state legislation and possible national legislation. If the Act is ineffective, proponents can point to the inefficiency and inconsistency of a state-by-state legislative approach when lobbying Congress.

PRACTICE POINTERS

For Manufacturers:

- Maintain and update records proving legal ownership and licensing agreements of all IT, regardless of whether the IT is used for manufacturing or other purposes.
- Work with clients to implement a code of conduct that establishes client expectations regarding IT licensing and use.
- Undertake or submit to routine auditing to ensure IT licensing compliance.

For Third Parties:

- Evaluate if the company can avoid liability by proving that (1) it is an end consumer or end user of the product being manufactured, (2) it has annual revenue of $50 million or less, or (3) it does not have a contractual relationship with the violating manufacturer.
- Send the violating manufacturer a letter demanding proof of compliance.
- Implement or update a manufacturer code of conduct and require all contracted manufacturers sign and adhere to the code.
- Implement or update supply chain management practices to effectively "scrub" the supply chain for stolen IT.