WHITE & CASE

The Emerging Risks of Unauthorized IP in Your Supply Chain and How You Should Respond

August 2013

Arthur M. Mitchell III
White & Case

Toshio Dokei
White & Case

Seiji Niwa
White & Case

Takako Onoki
White & Case

Pascal Berghe
White & Case

I. Introduction

Most global companies manage their supply chains to avoid supply disruptions and to address environmental, labor, and health and safety concerns, among others, but these same companies are often not aware of the significant legal and reputational risks of "Unauthorized IP" in their supply chains. Recent developments suggest that pursuit by the US federal government, state governments and private claimants, resulting in damages, injunctions and import restrictions, are increasingly likely. These are in addition to the risks from boycotts, reputational harm and from (potentially critical) suppliers dropping out of the market. This White Paper describes the various facets of this emerging threat, particularly in the United States but also in Europe and Japan, for companies with Unauthorized IP in their supply chains, and makes recommendations for how forward-looking companies can manage these risks. These risks are most acute in the United States but, as in other areas of law, other jurisdictions may follow the US lead in this area.

"Unauthorized IP" is intellectual property whose use has not been authorized by its lawful owner. This intellectual property can take a variety of forms, including patents, copyrights, utility models, software and trade secrets. It might include the unauthorized (and even inadvertent) use of unlicensed software in business processes or the use of misappropriated trade secrets. Although there may be a question in a specific case whether the use of IP was authorized or not, for the purposes of this White Paper we will assume that a violation of such IP rights by the suppliers can be proven to have taken place.

Problems with Unauthorized IP in the supply chain can affect even companies with rigorous IP compliance programs. The likelihood of a problem only increases when the Unauthorized IP in question is used not by the company or its subsidiaries but by its suppliers.

This paper first discusses the scope, magnitude and effects of Unauthorized IP in the global economy to make clear just how likely it is that companies, particularly those with their supply chains rooted in Asia, have Unauthorized IP in their supply chains. It then describes current and emerging risks in the United States under federal and state law, from the government and/or private plaintiffs. The situations in Europe and Japan are then explained. Other risks – boycotts and reputation harm specifically – are then addressed. The White Paper concludes with five measures that companies can take to help mitigate the increasing risks they face in this area.

II. The nature of the problem

Global companies often have deep and extensive supply chains. Companies are increasingly sensitive to the fact that their supply chains can pose significant risk to their operations. This point has been brought home recently by the impact of volcanic ash originating in Iceland in 2010,[1] flooding in Thailand the following year,[2] and, most markedly, in the tumult that followed the Great East Japan Earthquake.[3] Geopolitical developments can also be to blame.[4] Supply chain-related risks extend beyond simple supply disruptions to issues related to the environment, labor and labor standards, and health and safety concerns, among others. The effects can include disruption of business, litigation, reputational harm, and others, and may be as significant as injury (or even death) to consumers or the people working at factories linked to the supply chains.[5] Despite broad awareness of these supply chain risks, many companies do not yet seem to have the same concerns with respect to IP-related supply chain risk. It is, however, increasingly incumbent on them to treat these issues seriously.

Law-abiding companies would not permit their suppliers to use other forms of property whose use was not authorized in building their products. To take a (somewhat extreme) example: few companies would integrate components into their products that they know or should know to be stolen. They simply would not countenance having a supply chain that included companies who they know or should know were using stolen property in designing, producing, marketing or selling components. The same is not true, however, for Unauthorized IP. It seems that many more companies have not yet considered the risks associated with the integration of components comprised of or built or marketed using Unauthorized IP. But increasingly, both such companies and their suppliers may be open to charges that they are "beneficiaries of misconduct."[6]

III. Unauthorized IP in the global economy

A. Scope and Magnitude

A striking range of products and services are designed, produced, marketed and sold using Unauthorized IP. The range of IP-infringing products is virtually limitless and includes, inter alia, machinery and electrical equipment; metals and metal products; mineral products; chemical products; plastic and rubber; wood and wood products; pulp and paper products; textiles; stone, plaster, cement, ceramic and glass products; transportation equipment; optical and photo equipment; precision instrument;[7] non-physical content that does not include the use of physical media (such as music, movies, software) essentially used only over the internet,[8] and a host of other products.[9]

For example, OECD studies revealed the following infringing products in the automotive and the electrical components industry sectors:

Industry Sector	Examples of Products Subject to IP Infringement[10]
Automotive	Engines, engine parts, body panels, air bags, windscreens, tires, bearings, shock absorbers, suspension and steering components, automatic belt tensioners, spark plugs, disc brake pads, clutch plates, oil, filters, oil pumps, water pumps, chassis parts, engine components, lighting products, belts, hoses, wiper blades, grilles, gasket materials, rings, interior trim, brake fluid, sealing products, wheels, hubs, antifreeze, windshield wiper fluid
Electrical components	Components used in power distribution and transformers, switchgears, motors and generators, gas, and hydraulic turbines and turbine generator sets, relays, contacts, timers, circuit breakers, fuses, switchgears, distribution boards and wiring accessories, batteries

1 *Broken Links*, *The Economist* (Mar. 31, 2011), *available at* http://www.economist.com/node/18486015.

2 *Rising damp*, *The Economist* (Nov. 5, 2011), *available at* http://www.economist.com/node/21536652.

3 *Broken Links*, *The Economist*, *supra note 1*.

4 The Senkaku Islands dispute is a recent prominent example. *See, e.g., Rattling the Supply Chains, The Economist* (Oct. 20, 2012), available at http://www.economist.com/news/business/21564891-businesses-struggle-contain-fallout-diplomatic-crisis.

5 Steven Greenhouse, *Retailers Are Pressed on Safety at Factories*, N.Y. TIMES (May 10, 2013), available at http://www.nytimes.com/2013/05/11/business/global/clothing-retailers-pressed-on-bangladesh-factory-safety.html?pagewanted=all.

6 Andrew F. Popper, *Beneficiaries of Misconduct: A Direct Approach to IT Theft*, AM. CONST. SOC'Y FOR LAW & POL'Y ISSUE BRIEF (July 2012), http://www.acslaw.org/sites/default/files/Popper_-_Beneficiaries_of_Misconduct_0.pdf (using the term to describe companies who use "stolen" or "misappropriated" information technology).

7 OECD, *The Economic Impact of Counterfeiting and Piracy* 69 (2008) [hereinafter OECD 2008 Counterfeiting Report].

8 OECD, *Piracy of Digital Content 19* (2009) [hereinafter *OECD Digital Piracy Report*].

9 *OECD 2008 Counterfeiting Report*, *supra note 7*, at 69.

10 *Id.* at 68.

This striking list is only illustrative and "far from exhaustive."[11] Although many IP-infringing products are sold directly to consumers, others are sold to commercial entities and incorporated into goods for future sale.[12] Unauthorized IP may also be present in the supply chain as digital infringements of copyrights.[13] An example would be the use of unauthorized software in designing, producing, marketing and/or selling specific goods or even services. The scope of IP-infringing products is not only broad but likely expanding.[14] Surveys of customs officials indicate that Japan is among the countries where the range of counterfeit and pirated products is "expanding rapidly."[15]

The many companies with their supply chains rooted in Asia have reason to be particularly concerned, with the region fast emerging as the world's single largest producer of counterfeit and pirated products.[16] A significant percentage of the products sold in Asia are also believed to be counterfeit or pirated. For example, seven of the top twenty countries for pirated software sales (by commercial value) are in Asia: China, India, Indonesia, Japan, Malaysia, Sri Lanka and Thailand. China is the number two country globally on this list, with an estimated 77% of its software pirated.[17] That is, the value of pirated software in China is more than triple that of the value of legal sales. The rates of pirated software are strikingly high elsewhere in the region as well. Indonesia's rate, for example, is 86% and Thailand's is 72%. Japan's rate is 21% - the lowest of the countries in the region but actually marginally higher than that in the United States. Having a company in your supply chain that uses software that it is not licensed to use is, then, a real possibility.

Another possibility is that a supplier may hire a competitor's employee(s) – or use other means – to collect confidential information (including trade secrets) about that competitor. Similar practices are alleged to have taken place in a range of areas including prominently, in the last two years, para-aramid fiber (often more commonly referred to as Kevlar),[19] rubber resins and related manufacturing,[20] software for wind turbines[21] and cast steel railway wheels.[22] All four of these examples involved Asian companies. Such practices are not new but may now be taking place on an unprecedented scale.[23]

It is difficult to accurately calculate the value of stolen trade secrets across the global economy. Although this is also so for counterfeit and pirated goods, the OECD estimated that in 2007, the international trade in tangible counterfeit and pirated goods could be up to US$250 billion.[24] If counterfeit and pirated goods produced and consumed domestically and pirated digital products are included, the total value "could well be several hundreds of billions more."[25]

11 *Id.*

12 *Id.* at 315 (describing the electrical components sector).

13 *See generally*, OECD *Digital Piracy Report*, *supra* note 8.

14 *OECD 2008 Counterfeiting Report, supra* note 7, at 70.

15 *Id.*

16 *Id.* at 14.

17 Business Software Alliance, *Shadow Market: 2011 BSA Global Software Piracy Study 6* (9th ed. 2012), http://globalstudy.bsa.org/2011/downloads/study_pdf/2011_BSA_Piracy_Study-Standard.pdf.

18 *Id.*

19 *See E.I. DuPont de Nemours and Co. v. Kolon Indus., Inc.*, 894 F.Supp. 2d 691, 694-96 (E.D. Va. 2012) (summarizing the background and prior proceedings), stayed pending appeal by 2012 US App. LEXIS 20290 (4th Cir. Sept. 21, 2012).

20 *See Certain Rubber Resins & Processes for Mfg. Same*, Inv. No. 337-TA-849, Compl. Under Sec. 337 of the Tariff Act of 1930, as amended ¶ 19 (May 21, 2012).

21 Michael Riley & Ashlee Vance, *China Corporate Espionage Boom Knocks Wind out of US Companies*, BLOOMBERG, Mar. 15, 2012, *available at* http://www.bloomberg.com/news/2012-03-15/china-corporate-espionage-boom-knocks-wind-out-of-u-s-companies.html.

22 *See TianRui Grp. Co. v. Int'l Trade Comm'n*, 661 F.3d 1322, 1324 (Fed. Cir. 2011).

23 Riley & Vance, *Chinese Boom in Espionage, supra* note 21 (citing commonality of intellectual property theft and noting historical involvement of American, Russian, East German, Korean and Japanese companies in similar practices). Two strikingly egregious examples of such alleged conduct include that of Korean company Kolon Industries with respect to DuPont's Kevlar technology and China's Sinovel Wind Group with respect to American Superconductor Corp.'s wind turbine software. *See E.I. DuPont de Nemours and Co.*, 894 F.Supp. 2d 691; Riley & Vance, Chinese Boom in Espionage, supra note 21.

24 OECD, *Magnitude of Counterfeiting and Piracy of Tangible Products*: An Update 1 (2009).

25 *OECD 2008 Counterfeiting Report, supra* note 7, at 114.

B. Effects

The OECD identified numerous negative potential effects of counterfeit and pirated goods, including decreasing incentives to innovate and adversely affecting growth; increasing influence of criminal networks; and adverse impacts on the environment, employment, trade and foreign direct investment.[26] These broader socio-economic effects are in addition to the obvious negative impact on rights holders, government (including in the form of decreased tax revenues) and consumers (including health and safety risks).[27]

The use of Unauthorized IP also gives companies an unfair business advantage. This is true both of infringing companies themselves and those companies who have Unauthorized IP in their supply chains. Companies who use or have Unauthorized IP in their supply chains have a lower cost structure than their law-abiding competitors – in effect an unearned competitive advantage. This concern is also at the heart of many of the laws and policies discussed below.

IV. Major Legal Risks

A. US Federal Law

A company's first broad areas of concern in this area are under US federal law. The mechanisms for enforcement, particularly by the federal government, are in some cases still coming into focus, but there are indications of a trend towards increased concern with the US import and sale of products containing Unauthorized IP.

At the federal level, there are two primary areas of concern for a company with Unauthorized IP in its supply chain: (i) enforcement by the Federal Trade Commission (the "FTC") and (ii) Section 337 of the Tariff Act of 1930 ("Section 337"),[28] claims under which can be pursued by the US International Trade Commission (the "ITC") itself or by private parties. The FTC may be moving towards taking action (although the precise mechanism of that enforcement remains uncertain), while enforcement actions relevant to Unauthorized IP under Section 337 has already taken place.

Issues related to Unauthorized IP have been recognized by officials at the top of the US government, including then-Secretary of State Clinton and even President Obama himself, who have noted these as priorities.[29] In a widely covered speech in October 2011, then Secretary Clinton referred specifically to the policing of supply chains and stated that she was "encouraged that a new coalition of major companies is coming together to keep global supply chains free of pirated software and counterfeit goods."[30] She cited this as ensuring that innovators receive "their rightful reward" and as creating American jobs.[31] Following a commitment in the 2012 State of the Union address to tackle unfair trade practices by foreign countries, President Obama ordered the creation of the Interagency Trade Enforcement Center ("ITEC"). ITEC is to "coordinate and augment" the activities of executive departments and agencies "to identify and reduce or eliminate foreign trade barriers and unfair foreign trade practices."[32] This explicitly includes enforcement of "domestic trade laws" and "trade rights involving intellectual property rights."[33] Whether ITEC will pursue the use of Unauthorized IP in foreign supply chains remains to be seen but such issues clearly fall within its purview.

26 *Id.* at 135-41.

27 *Id.*

28 19 USC. § 1337 (2012).

29 President Barack H. Obama, US President, State of the Union Address (Jan. 24, 2012), *available at* http://www.whitehouse.gov/the-press-office/2012/01/24/remarks-president-state-union-address ("And I will not stand by when our competitors don't play by the rules...Tonight, I'm announcing the creation of a Trade Enforcement Unit that will be charged with investigating unfair trade practices in countries like China. There will be more inspections to prevent counterfeit or unsafe goods from crossing our borders."); Hilary R. Clinton, US Sec'y of State, On Economic Statecraft, Address at the Economic Club of New York (Oct. 14, 2011), *available at* http://iipdigital.usembassy.gov/st/english/texttrans/2011/10/20111014172924su0.9650494.html#ixzz2KxUlqmb4 ("In the 1990s, businesses used their supply chains to take on the problem of child labor in the developing world, and it was American businesses that began to change the terrible picture of five-, seven-, nine-year-old children in what amounted to forced labor. Today, I am encouraged that a new coalition of major companies is coming together to keep global supply chains free of pirated software and counterfeit goods. That gives innovators their rightful reward, but it also creates American jobs. Because nobody outworks us, and nobody out-innovates us. We just have to be out there competing to deliver what we do best.").

30 Clinton, *supra* note 29.

31 *Id.*

32 Exec. Order No. 13601, 3 C.F.R. 220, 220 (2012).

Indeed, IP theft is an issue of increasing importance on the national agenda in the United States. In 2012, General Keith Alexander, chief of the United States Cyber Command and the director of the National Security Agency, called the loss of industrial information and intellectual property through cyberspace "the greatest transfer of wealth in history."[34] On May 7, a bipartisan group of prominent senators introduced a bill called the "Deter Cyber Theft Act."[35] Under the Act, the Director of National Intelligence ("DNI") would prepare an annual report on foreign economic and industrial espionage that includes: (1) a list of foreign countries that engage in economic or industrial espionage in cyberspace against US firms or individuals, including a priority watch list of the worst offenders; (2) a list of US technologies or proprietary information targeted by such espionage, and, to the extent possible, a list of such information that has been stolen; (3) a list of items produced using such stolen information; (4) a list of foreign companies, including state-owned firms, that benefit from such theft; (5) details of the espionage activities of foreign countries; and (6) actions taken by the DNI and other federal agencies to combat industrial or economic espionage in cyberspace. The US President could then block the importation of "products containing stolen US technology; products made by state-owned enterprises of nations on the Director of National Intelligence's priority watch list that are similar to items identified in the DNI's report as stolen or targeted US technology; or made by a company the DNI identifies as having benefited from theft of US technology or proprietary information."[36] The Deter Cyber Theft Act would, if passed, join laws like the Economic Espionage Act ("EEA") in the federal IP theft enforcement toolbox.[37]

Enforcement Risk 1: Federal Trade Commission

To date, the FTC has not yet taken significant enforcement action to combat the use of Unauthorized IP. The agency is under pressure, however, to address the issue and is considering enforcement options. The FTC should be watched closely, as it may begin pursuing such activity, either as part of a broader antitrust case or on its own as an unfair method of competition.

In November 2011, the National Association of Attorneys General ("NAAG"), which is comprised of the chief legal officers of US states, commonwealths and territories, urged the FTC to consider using its powers under Section 5 of the Federal Trade Commission Act ("FTC Act") to address information technology theft.[38] This letter was followed several months later by letters from the US Senate Committee on Small Business & Entrepreneurship and the US House of Representatives Committee on Small Business, both encouraging action by the FTC in this area.[39] The former referred not just to IT theft but also to intellectual property

33 *Id.* at 220, 221. Note that Section 337 of the Tariff Act of 1930, which is discussed further below, is explicitly included under the Order's definition of "domestic trade laws" in section 5(b). Id. at 222.

34 *See, e.g.,* David E. Sanger & Mark Landler, *US and China Agree to Hold Regular Talks on Hacking*, N.Y. TIMES (Jun. 1, 2013), available at http://www.nytimes.com/2013/06/02/world/asia/us-and-china-to-hold-talks-on-hacking.html?pagewanted=all&_r=0.

35 See Press Release, Office of Sen. Carl Levin (Mich.), Bipartisan Group of Senators Introduces Legislation to Combat Cyber Theft (May 7, 2013), http://www.levin.senate.gov/newsroom/press/release/bipartisan-group-of-senators-introduces-legislation-to-combat-cyber-theft.

36 *Id.* According to the draft bill, the President would exclude from importation certain statutorily-defined IP theft-related products if he "determines the exclusion of the article is warranted...for the enforcement of intellectual property rights; or...to protect the integrity of the Department of Defense supply chain." S. 884, 113th Cong. § 2(b) (2013).

37 Economic Espionage Act, 18 USC. §§ 1831-32 (2012), makes it a federal crime to steal trade secrets either for pecuniary gain or for the benefit of a foreign entity. The EEA explicitly includes theft from electronic storage. *See, generally*, Charles Doyle, Cong. Research Serv., R42681, *Stealing Trade Secrets and Economic Espionage: An Overview of 18 USC. 1831 and 1832*, at 1 (2013), *available at* http://www.fas.org/sgp/crs/secrecy/R42681.pdf. In 2012, the EEA was twice updated. First, 18 USC. 1832(a) was amended to close a jurisdictional loophole through the passage of Theft of Trade Secrets Clarification Act, Pub. L. No. 112-236, 126 Stat. 1627 (2012). Second, 19 USC. 1831(a) & (b) were amended to increase the fine levels for economic espionage and to direct the US Sentencing Commission to reevaluate economic espionage and the overseas transmission of stolen trade secrets under the US Sentencing Guidelines through the passage of the Foreign and Economic Espionage Penalty Enhancement Act of 2012, Pub. L. No. 112-269, ¶¶ 2-3, 126 Stat. 2442, 2442-43 (2013). For a detailed discussion of both amendments, see Doyle, *Stealing Trade Secrets* at 13-15. An additional example of the rising prominence of this issue is a recent report by the private Commission on the Theft of American Intellectual Property. *See* Comm'n on the Theft of Am. Intellectual Prop., The IP Commission Report (2013), *available at* http://www.ipcommission.org/report/IP_Commission_Report_052213.pdf. This Commission, which includes the former Director of National Intelligence and the former Ambassador to China, among other "leading Americans from the private sector, public service in national security and foreign affairs, academe, and politics," released a report in which they discussed the theft of US intellectual property, and proposed strong possible responses. Id. at 1; *see also* David Sanger, As Chinese Leader's Visit Nears, US is Urged to Allow Counter Attacks on Hackers, N.Y. TIMES (May 21, 2013), *available at* http://www.nytimes.com/2013/05/22/world/asia/as-chinese-leaders-visit-nears-us-urged-to-allow-retaliation-for-cyberattacks.html?pagewanted=all.

38 Letter from National Association of Attorneys General to FTC Commissioners and Director of Bureau of Competition (Nov. 11, 2011); 15 USC. § 45 (2012).

39 Letter from US Senate Committee on Small Business and Entrepreneurship to FTC Commissioners (Apr. 2, 2012); Letter from US House of Representatives Committee on Small Business to FTC Commissioners (Aug. 2, 2012).

40 US Senate Committee Letter to FTC Commissioners, *supra* note 39 ("We are writing you to ask you to consider a request submitted by the National Association of Attorneys General (NAAG) to use all the tools at your disposal to fight the theft and use of stolen American manufacturing information technology (IT) and intellectual property (IP).").

41 NAAG also cites specific examples of the cost disadvantages faced by law-abiding companies. *See, e.g.*, NAAG Letter to FTC Commissioners, *supra* note 38 (citing the following examples: "A California-based apparel manufacturer must compete with an Indian manufacturer that steals over US$14 million in software," "A Washington-based paper mill must compete with a Mexican paper manufacturer that uses over US$10 million in stolen software," and "An Indiana-based parts manufacturer must face a Chinese competitor that steals over US$5.2 million in software").

more broadly.[40] All three letters note that such unfair uses allow law-violating companies to lower their costs in competing with law-abiding American companies.[41] They further link this unfair conduct by foreign competitors with the decline in manufacturing in the United States. The New York State Senate also passed a resolution "memorializing the President, the Federal Trade Commission and the United States Congress to strictly enforce United States trade laws to protect domestic information technology and intellectual property rights and address unfair competition in the marketplace generated by the institutionalized theft of information technology and intellectual property."[42]

Section 5 of the FTC Act prohibits "unfair or deceptive acts or practices in or affecting commerce,"[43] and gives the FTC potentially broad enforcement authority over all manner of unfair and deceptive conduct. The FTC can seek injunctive and other equitable relief, including redress, for violations. It may also seek civil penalties from a person or company that knowingly violates its rules relating to unfair and deceptive acts or practices.[45]

The FTC has yet to take action in this area and statements by FTC Commissioners may suggest some hesitancy to use Section 5 to effect enforcement in this area. However, the then-FTC Chairman said that he shares these concerns about foreign companies gaining an unfair advantage when they use stolen IT and IP in competition with American firms that follow the law.[46] He notes that such conduct could "distort competition," "stifle incentives for innovation and growth," and "lead to the loss of American manufacturing and other jobs."[47] He further indicated that Section 5 enforcement authority might indeed be available to address these issues. The FTC has thus said that it will begin a dialogue with the NAAG, "to explore whether the use of the FTC's tools, including Section 5 enforcement authority, may be appropriate to address these issues."[48] This discussion was to include consideration of whether collaboration between the FTC and the states would be productive.[49]

Given the focus of the NAAG and Congressional committees on the difficulties facing US manufacturers, it is reasonable to assume that the risks of enforcement action in this area may be higher for companies that compete directly with US manufacturers. This is particularly so in industries where the US manufacturers are having difficulty competing with their foreign competitors. Furthermore, there do not appear to be any significant policy reasons that would prevent the FTC from using Section 5 as an enforcement mechanism.[50]

Enforcement Risk 2: Section 337 of the Tariff Act of 1930

Under the aegis of Section 337 of the Tariff Act of 1930, a company and its suppliers could also face an investigation by the ITC or a private complaint in connection with Unauthorized IP.[51] An adverse finding by the ITC can result in a ban on imports into the United States of the supplier's infringing component itself or even of a company's downstream products that incorporate the infringing component. In addition, an adverse judgment would be persuasive authority in a related federal court action, which could result in damages.

42 S. K-1544 (N.Y. 2012).

43 15 USC. § 45(a)(1).

44 Section 5 of the FTC Act has been found by courts to be broader than the prohibitions under Section 1 (concerted conduct) and Section 2 (unilateral conduct) of the Sherman Antitrust Act. *See, e.g., FTC v. In. Fed'n of Dentists*, 476 US 447, 454 (1986) (Section 5 of the FTC Act encompasses "practices that violate the Sherman Act and other anitrust laws."). *See also* ABA Section of Antitrust Law, ANTITRUST LAW DEVS. 660 (7th ed. 2012) ("…the scope of Section 5 is at least as broad as that of the Sherman, Clayton and Robinson-Patman Acts combined.").

45 15 USC. § 45(m)(1)(A) (allows FTC to seek civil penalties from a company or person violating any such rule "with actual knowledge or knowledge fairly implied on the basis of objective circumstances that such act is unfair or deceptive and is prohibited by such rule.").

46 Letter from Jon Leibowitz, Chairman, FTC to Mary L. Landrieu, Chair, US Senate Committee on Small Business and Entrepreneurship (Apr. 6, 2012). Note that Chairman Leibowitz exited the FTC in February. It remains to be seen whether and how his successor will address these issues.

47 *Id.*

48 *Id.*

49 *Id.*

50 As recently pointed out by William Kovacic, a prominent commentator and former FTC Chairman, misappropriation of IP has featured prominently in past FTC Section 5 cases and fits squarely within the statute's original intent. William Kovacic, Comments at A.B.A. Section of Antitrust Law Event: *Battling IT Theft and Unfair Competition: Enforcers Use A New Approach* (June 26, 2013). He also noted that a successful case for IT theft might be brought under Section 5 given that it is serious misconduct and that it is difficult to imagine an offsetting pro-competitive rationale. Id.

51 19 USC. § 1337 (2012).

Section 337 prohibits "unfair methods of competition and unfair acts in the importation of articles…into the United States, or in the sale of such articles by the owner, importer, or consignee" that threaten to or have the effect of "destroy[ing] or substantially injur[ing] an industry," "prevent[ing] the establishment of such an industry" or "restrain[ing] or monopoliz[ing] trade and commerce in the United States."[52] Further, this provision authorizes the ITC to exclude from importation any article that violates US IP rights, including those involving patents,[53] copyrights,[54] trademarks[55] and design rights.[56] Enforcement action has also been taken in connection with a range of other conduct, including misappropriation of trade secrets.[57] Although this provision has broader application (e.g., to antitrust claims and false advertising) it is most often used for claims involving IP rights.[58]

Section 337 has been interpreted as being applicable to misappropriation of trade secrets occurring outside the United States when the products produced through the misappropriation were imported to the United States.[59] Thus, Section 337 could be applicable to the conduct of a company and/or its suppliers even though the misappropriating acts took place abroad. Recent developments suggest that Section 337 actions based on alleged misappropriation of trade secrets may be becoming more commonplace.[60]

If the ITC finds a Section 337 violation, it can issue an "Exclusion Order," directing US Customs and Border Protection to exclude the infringing products from the United States.[61]

Such an order may either be a Limited Exclusion Order (or "LEO") or a General Exclusion Order (a "GEO"). The latter is applicable to downstream products from non-respondents that incorporate IP-infringing components, regardless of the source of the goods, their manufacturer or their importer.[62] Unlike a LEO, a GEO applies to non-parties.[63] A GEO, however, requires a substantially higher burden of proof than a LEO.[64]

The ITC may also issue a "Cease and Desist Order," directing the violating parties to cease certain actions.[65] Cease and desist orders are often issued concurrently with an exclusion order.[66] Expedited relief is also available under exceptional circumstances. Section 337 investigations include trial proceedings before administrative law judges and review by the Commission. Commission decisions are appealable to the Court of Appeals for the Federal Circuit.

Section 337 proceedings may be initiated by the ITC itself but are typically commenced pursuant to complaints brought to it by affected private parties. Both US competitors and the holders of IP (such as the IP holder of the software that a supplier is using unlicensed) would have incentives to do so. The filing of a private ITC action is often coupled with the commencement of an action in federal district court. Although damages are not available in an ITC case, they are available in the related federal court case. Typically, the federal court action will be stayed pending resolution of the ITC action, with that stay lifted after the ITC case. The ITC judgment will be persuasive – but not binding – authority in federal court.

52 *Id.* at § 1337(a)(1)(A).

53 *Id.* at § 1337(a)(1)(B)(i).

54 *Id.*

55 *Id.* at § 1337(a)(1)(C).

56 *Id.* at § 1337(a)(1)(E).

57 *See, e.g.*, USITC, *Intellectual Property Infringement and Other Unfair Acts*, http://www.usitc.gov/intellectual_property/ (last visited July 18, 2013); *TianRui Grp. Co. Ltd. v. Int'l Trade Comm'n*, 661 F.3d 1322, 1323-24 (Fed. Cir. 2011).

58 *See, e.g.*, USITC, *supra* note 56; Popper, *supra* note 6, at 8 (citing S. Rep. No. 100-71, at 128 (1987)) ("Congress has stated that the language of [Section] 337 'is designed to cover a broad range of unfair acts.'").

59 See *TianRui Grp.*, 661 F.3d at 1332.

60 *See* Certain Electric Fireplaces, Components Thereof, Manuals for Same, and Products Containing Same, Certain Processes for Manufacturing or Relating to Same, and Certain Prods. Containing Same, Inv. Nos. 337-TA-791, 337-TA-826 (Jan. 13, 2012) (Active); Certain Rubber Resins and Processes for Mfg. Same, Inv. No. 337-TA-849 (Jun. 26, 2012) (Active).

61 19 USC. § 1337(d)-(e), (g).

62 *See Kyocera Wireless Corp. v. Int'l Trade Comm'n*, 545 F.3d 1340, 1358 (Fed. Cir. 2008); *Fuji Photo Film Co. v. Int'l Trade Comm'n*, 474 F.3d 1281, 1286 (Fed. Cir. 2007); *See also* Bas de Blank & Bing Cheng, *Where is the ITC Going after Kyocera?*, 25 SANTA CLARA COMPUTER & HIGH TECH. L.J. 701, 704–05 (2009).

63 *Fuji Photo*, 474 F.3d at 1286.

64 GEOs are only issued where the Commission finds that (1) the GEO is "necessary to prevent the circumvention of an exclusion order limited to products of named persons"; or (2) "there is a pattern of violation...and it is difficult to identify the source of the infringing products." 19 USC. § 1337 (d)(2).

65 19 USC. § 1337 (f)-(g).

66 de Blank & Cheng, *supra* note 61, at 705.

ITC enforcement actions can affect not just a party infringing IP but also importers of that IP into the United States and importers of downstream products that incorporate the infringing component. Until 2008, it was the ITC's long-standing practice to include within the scope of its LEOs not just the infringing products themselves but also the downstream products into which infringing components were incorporated manufactured by third parties who were not named as respondents to the ITC investigation. Although a 2008 US Court of Appeals decision[67] imposed limitations on this practice, there is still scope to pursue downstream products that incorporate infringing components, either by seeking a GEO or by naming all known respondents in the first instance.

B. US State Laws

Companies and their suppliers may also be subject to claims under US state laws. State enforcement action in connection with Unauthorized IP has already taken place in some states and in others, claims may already be viable under existing state "unfair or deceptive practices" business laws. Further, state statutes have recently been passed specifically targeting the unauthorized use of information technology and these are only expected to grow in number.

The NAAG letter to the FTC signals the seriousness with which state enforcers already see the use of unauthorized IT by foreign companies competing in the US market. As noted above, the attorneys general who sent a letter to the FTC seeking enforcement by that agency specifically cited the impact of such unfair conduct on US manufacturers. NAAG also addressed these issues at a panel discussion at its summer meeting in 2013.[68] In a session entitled "Enforcement against Unfair Competition Arising from Stolen Intellectual Property," enforcers and former enforcers from California, Massachusetts and Washington discussed enforcement efforts by their offices and encouraged other attorneys general to consider what steps their offices could take in this area.[69]

Non-US companies competing directly with US manufacturers, particularly those US manufacturers losing market share to their foreign competition, are likely to be particularly at risk of facing enforcement. Many state statutes also enable private claims.

This section discusses two categories of risks in these areas: (i) state laws with provisions specifically governing unauthorized IT; and (ii) state unfair and deceptive practices legislation.

Enforcement Risk 3: State Laws Governing Unauthorized Information Technology

In the past three years, the states of Washington and Louisiana have adopted statutes specifically addressing the unauthorized use of information technology. At least twelve other states, including California and New York, have taken the step of introducing similar legislation, although these have thus far not been adopted.

The use of unauthorized IT is a commonly occurring subset of Unauthorized IP, and companies should be aware that there is a significant likelihood of suppliers using unauthorized IT. This is particularly so in Asia. As noted above, seven of the top twenty countries for pirated software sales (by commercial value) are in Asia: China, India, Indonesia, Japan, Malaysia, Sri Lanka and Thailand. An estimated 77% of the software in China is pirated, as is 86% of the software in Indonesia.[70] These unauthorized uses of IT may even extend to state-owned enterprises.[71]

Washington State – Unfair Competition Law, § 19.330 et seq. & La. Rev. Stat. Ann. § 51:1427

Washington State added a provision to its Unfair Competition Law regarding "Stolen or Misappropriated Information Technology."[72] This new provision, which went into effect in July 2011, makes the unauthorized use of hardware and software by product manufacturers in the manufacturing, production or assembly of tangible products sold in the state an "unfair act" subject to penalty. Potential liability is extended not only to parties that

67 *See Kyocera Wireless Corp. v. Int'l Trade Comm'n*, 545 F.3d 1340 (Fed. Cir. 2008).

68 Nat'l Assoc. of Att'ys Gen'l, 2013 Summer Meeting Agenda, *Privacy in the Digital Age: Preparing Your Team For Solutions Online and Offline*, http://www.naag.org/assets/files/pdf/meetings/2013_summer/2013%20Summer%20Meeting%20Agenda.pdf (last visited July 18, 2009) (see June 18, 2013 agenda).

69 Video of this session is available on the NAAG website at http://www.naag.org/tuesday-june-18-2013.php.

70 *BSA Global Software Piracy Study, supra* note 17, at 6.

71 *See Microsoft Said to ask China to Stop Piracy at Four Firms*, BLOOMBERG BUS. WEEK (Sep. 20, 2012), *available at* http://www.businessweek.com/news/2012-09-20/microsoft-said-to-ask-china-to-stop-piracy-at-four-state-firms (citing possible widespread use of unauthorized IT at state-owned enterprises).

72 WASH. REV. CODE § 19.330 (2011).

have directly used the Unauthorized IP but also to certain third parties incorporating misappropriated IP into products sold into Washington state. The Washington state statute does, however, include important safe harbors and affirmative defenses.

Notably, the unauthorized IT at issue does not need to be incorporated into the product sold in Washington state; for these purposes it is sufficient for liability under the law if the IT is used in business operations (such as distribution, sales and marketing, inventory, logistics and accounting). Thus a supplier's illegal use of software in its business operations would put the supplier – and potentially the company that relies on that supplier in its supply chain – squarely in the law's crosshairs. Sellers into Washington state should thus be careful to police their supply chains for Unauthorized IP.

Possible sanctions include: (1) seizure of products; (2) injunction against sales; and/or (3) damages, up to and including treble damages for willful conduct by the direct violator. Enforcement is by both the Washington Attorney General and by private party competitors who meet certain requirements. Third parties can potentially be sued where the competitor cannot collect damages directly from the direct violator of the law (i.e., the violating supplier) or in an in rem action (i.e., an action against the products themselves). In order for a third party to liable, they must also be in a contractual relationship with the direct violator and either be the seller of the direct violator's final product or include in the final product a component from the direct violator valued at more than 30% of the final product's value. The law also exempts certain categories of products, notably including those that involve alleged patent infringement or stolen trade secrets.

The Washington state law was preceded by a similar law passed in Louisiana in 2010.[73] The key differences between the two laws are (1) the latter's simplicity (the Washington state law has a more complex legal framework); and (2) the Louisiana law is applicable not just to products but to services as well. Under the Washington law, damages are the primary remedy against suppliers. These may be either actual direct damages or statutory damages equivalent to the "retail price" of the IT in questions. Treble damages may also be assessed where the use was found to be willful. If a judgment cannot be satisfied because of the absence of attachable assets in Washington to satisfy the judgment, an injunction may also be possible.[74] Remedies are also available, under certain circumstances, against the products themselves (such as through attachment) and damages claims are also available (under certain circumstances) against third parties with more than US$50 million in annual revenues who offer to sell the offending products and have a direct contractual relationship with the party involved in the infringement. There are certain situations where a plaintiff can also seek damages from a third party where the manufacturer fails to appear or does not have adequate assets to satisfy a judgment.

The threat of an action under the Washington State law has already been used to exact a settlement from a company that was using Unauthorized IP. In April 2013, the state Attorney General announced that Microsoft had reached a settlement with Embraer, a Brazilian company and the world's fourth-largest aircraft manufacturer, regarding the company's "under-licensing" of software.[75] This settlement, which was for US$10 million, was for the company's alleged licensed use of ten proper Microsoft licenses for 3,300 installations of that software. The Attorney General's office "exchanged several letters with the Brazilian company in an effort to resolve this matter before taking more formal steps."[76]

Other States

In addition to Washington and Louisiana, a number of other states have introduced similar legislation for consideration. These states include: Arizona, California, Connecticut, Illinois, Indiana, Kentucky, Massachusetts, Missouri, New York, North Carolina, Oregon and Utah. Although such efforts have not proven successful thus far, developments in these states should be carefully monitored, as they may raise further compliance considerations for companies that sell into the affected states.

73 LA. REV. STAT. ANN. § 51:1427 (2012).

74 The rules governing injunctions differ depending on whether a private plaintiff or the government is involved.

75 *See* Press Release, Wash. State Off. of the Att'y Gen., *Washington's New Unfair Competition Law Protects Local Company from Software Privacy: Embraer, World's 4th Largest Aircraft Manufacturer, Now in Full Compliance* (Apr. 3, 2013), *available at* http://www.atg.wa.gov/pressrelease.aspx?id=31143; Brian T. Moran, Chief Deputy, Wash. State Off. of the Att'y Gen., *Embraer Aircraft*, Presentation at the 2013 NAAG Summer Meeting (June 18, 2013), *available at* http://www.naag.org/assets/files/pdf/meetings/2013_summer/TUE/Moran.Embraer%20Aircraft.pdf.

76 *Embraer* Press Release, *supra* note 75.

Enforcement Risk 4: State Unfair and Deceptive Acts & Practices Laws

Companies may also face risks under state unfair and deceptive acts and practices legislation (hereafter "UDAP statutes"). At least two states, Massachusetts and California, have already used their UDAP statutes to pursue companies for their unauthorized use of IP. Both states did so even though the final products sold into the state did not include the Unauthorized IP as an integrated component. This suggests that specific IP-related legislation need not be in place for similar enforcements to be replicated in other states but that general consumer protection laws can achieve the same outcome. These state laws arguably pose one of the greatest risks to companies and their global suppliers, for a number of reasons. First, these laws are often quite broad, capable of encompassing a broad range of unfair competitive conduct. Although Massachusetts and California have pursued actions involving the use of pirated IT by direct suppliers of products (i.e., they have not yet pursued a company that does not itself use Unauthorized IP but includes it in its supply chain), the reasoning that the two states have used – that the foreign companies' conduct gives them an unfair competitive advantage vis-à-vis their law-abiding US competitors – applies equally to IP as well as the narrower category of IT and can apply with near equal force to indirect beneficiaries of Unauthorized IP as it can to the unauthorized users themselves. The penalties can also seriously impact business; even where the financial penalties assessed are modest, an injunction preventing the sale of certain products in a given state could be very disruptive. Finally, the number of jurisdictions involved effectively multiplies these challenges.

State UDAP laws can cover a very broad range of conduct that can, in many instances, be likely to include certain uses of Unauthorized IP. Although all of the fifty states and the District of Columbia have UDAP statutes,[78] there are significant differences among the various laws. The UDAP laws include either a prohibition on "unfair practices," a prohibition on "deceptive practices," or both.[79] Often these prohibitions are broad and general, with their scope not limited to specific, enumerated practices but instead accommodating a range of unfair and/or deceptive conduct. The FTC Act, on which many of the UDAP statutes are based, takes the same approach. The statutes most likely to encompass the Unauthorized IP-related conduct described above are those with broad unfairness/unconscionability prohibitions. Claims are less likely to be successful where the statute only prohibits "deceptive" practices, particularly where those practices are enumerated.

77 *See* S. 1529, 15th Leg., 1st Reg. Sess. (Ariz. 2011); Assemb. 473, 2011 Leg., Reg. Sess. (Cal. 2011) (died pursuant to Art. IV, Sec. 10(c) of Const.); H.R. 6619, 2011 Gen. Assemb., Jan. Sess. (Conn. 2011); S. 1861, 97th Gen. Assemb., 2011-12 Sess. (Ill. 2011); S. 529, 117th Gen. Assemb., 1st Reg. Sess. (Ind. 2011); H.R. 113, 2011 Gen. Assemb., Reg. Sess. (Ky. 2011); H.R. 2842, 187th Gen. Court, 2011 Sess. (Mass. 2011); H.R. 1022, 96th Gen. Assemb., 1st Reg. Sess. (Mo. 2011); Assemb. 3915, 2011 Assemb., Reg. Sess. (N.Y. 2011) (held for consideration in Econ. Deb. Comm.); S. K-1544 (N.Y. 2012); H.R. 672, 2011 Gen. Assemb., Reg. Sess. (N.C. 2011); H.R. 3315, 76th Leg. Assemb., 2011 Reg. Sess. (Or. 2011); S. 201, 2011 Gen. Sess. (Utah 2011).

78 *See* ALA. CODE §§ 8-19-1 to 8-19-15 (1981) (Alabama); ALASKA STAT. §§ 45.50.471 to 45.50.561 (1970); ARIZ. REV. STAT. ANN. §§ 44-1521 to 44-1534 (1967) (Arizona); ARK. STAT. ANN. §§ 4-88-101 to 4-88-115 (1971) (Arkansas); CAL. CIV. CODE §§ 1750 to 1784 (1970), and CAL. BUS. & PROF. CODE §§ 17200 to 17209 (1977) (California); COL. REV. STAT. §§ 6-1-101 to 6-1-1001 (1969) (Colorado); CONN. GEN. STAT. §§ 42-110a to 42-110q (1973 (Connecticut); DEL. CODE ANN. tit. 6, §§2501 to 2597 (1953) (Delaware); D.C. CODE ANN. §§ 28-3901 to 28-3913 (1973) (District of Columbia); FLA. STAT. ANN. §§501.201 to 501.976 (1973) (Florida); GA. CODE ANN. §§ 10-1-370 to 10-1-438 (1975) (Georgia); HAWAII REV. STAT. §§ 480-1 to 480-24 (1961), and HAWAII REV. STAT. §§ 481A to 481B; and 487-1 to 487-16 (1969); IDAHO CODE §§ 48-601 to 48-619 (1971); ILL. REV. STAT. ch. 815, §§ 505 to 601 (1961) (Illinois); IND. CODE ANN. §§ 24-5-0.5 to 24-5-0.5-12 (1971) (Indiana); IOWA CODE ANN. §§ 714.16 to 714.26, 714A, 714B, 714D, 714H (1966); KAN. STAT. ANN. §§ 50-623 to 50-6107 (1973) (Kansas); KY. REV. STAT. §§ 367.110 to 367.993 (1972) (Kentucky); LA. REV. STAT. ANN. §§ 51:1401 to 51:142& (1972) (Louisiana); ME. REV. STAT. ANN. tit. 5, §§ 205A to 214, and tit. 10, §§ 1211 to 1216 (1969) (Maine); MD. COM. LAW CODE ANN. §§ 13-101 to 13-501 (1975) (Maryland); MASS. GEN. LAWS ANN. ch. 93A §§ 1 to 11 (1967); MICH. COMP. LAWS. §§ 445.901 to 445.922 (1977) (Michigan); MINN. STAT. ANN. §§ 325D.09 to 325D.16 (1943), 325D.43 to 325D.48 (1973), and 325F.67 to 325F.99, 325G (1973) (Minnesota); MISS. CODE ANN. §§ 75-24-1 to 75-24-175 (1974) (Mississippi); MO. REV. STAT. §§ 407.010 to 407.1355 (1967) (Missouri); MONT. CODE ANN. §§ 30-14-101 to 30-14-143 (1973) (Montana); NEB. REV. STAT. §§ 59-1601 to 59-1623, and 87-301 to 87-306 (1974) (Nebraska); NEV. REV. STAT. §§ 598.0903 to 598A.280 (1973) (Nevada); N.H. REV. STAT. ANN. §§ 358-A:1 to 358-A:13 (1970) (New Hampshire); N.J. STAT. ANN. §§ 56:8-1 to 56:8-184 (1960) (New Jersey); N.M. STAT. ANN. §§ 57-12-1 to 57-12-26, 12B (1967) (New Mexico); N.Y. GEN. BUS. LAW §§ 349 to 350-f-1 (1970) (New York); N.C. GEN STAT. §§ 75-1 to 75-135 (1969) (North Carolina); N.D. CENT. CODE §§ 51-15-01 to 51-15-11 (1965) (North Dakota); OHIO REV. STAT. ANN. §§ 4165.01 to 4165.04 (1972), and 1345.01 to 1345.99 (1971); OKLA. STAT. ANN. tit. 15, §§ 751 to 799 (1972), and tit. 78, §§ 51 to 56 (1971) (Oklahoma); OR. REV. STAT. §§ 646.605 to 646.656 (1965) (Oregon); PA. STAT. ANN. tit. 73, §§ 201-1 to 210-6 (1968) (Pennsylvania); R.I. GEN. LAWS §§ 6-13.1-1 to 6-13.1-28 (1968) (Rhode Island); S.C. CODE §§ 39-5-10 to 39-5-170 (1962) (South Carolina); S.D. CODIFIED LAWS ANN. §§ 37-24-1 to 37-24-48 (1971); TENN. CODE ANN. §§ 47-18-101 to 47-18-5541 (1977) (Tennessee); TEX. BUS. & COM. CODE ANN. §§ 17.01 to 17.926 (1973) (Texas); UTAH CODE ANN. §§ 13-11-1 to 13-11-23 (1973); VT. STAT. ANN. tit. 9, §§ 2451 to 2480r (1967) (Vermont); VA. CODE §§ 59.1-196 to 59.1.207 (1977) (Virginia); WASH. REV. CODE §§ 19.86.010 to 19.86.920 (1961) (Washington); W. VA. CODE §§ 46A-6-101 to 46A-7-115, and 46A-7-101 to 46A-7-115 (1974) (West Virginia); WIS. STAT. §§ 100.01 to 100.60 (1921) (Wisconsin); and WYO. STAT. §§ 40-12-101 to 40-12-509 (1973) (Wyoming) (*as cited in* Mary Dee Pridgen, *Consumer Protection and the Law*, App 3A (database updated November 2012)).

79 According to a 2009 report, the UDAP statutes of thirty-nine states and the District of Columbia include "at least a fairly broad prohibition against unfair or unconscionable acts" that can be enforced by a state agency and consumers. Carolyn L. Carter, Consumer Protection in the States: A 50-State Report on Unfair and Deceptive Acts and Practices Statutes, NAT'L CONSUMER L. CTR. INC. 12 (Feb. 2009), available at http://www.nclc.org/images/pdf/car_sales/UDAP_Report_Feb09.pdf. Forty-three states and the District of Columbia include in their UDAP statute a broad prohibition on "deception" enforceable by both a state agency and consumers. Id. at 11.

The Narong Seafood case, which was brought in Massachusetts, falls within the first category: Massachusetts General Law Chapter 93A, the state's Consumer Protection Law, broadly prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade commerce," but does not include a definitive list of prohibited practices.[80] In October 2012, the Massachusetts Attorney General fined Narong, a Thailand-based seafood processer,[81] US$10,000 for violating Massachusetts Chapter 93A.[82] The fine was for the company's failure to pay licensing fees for software that it used to sell and produce its products. This case is the first of its type under Massachusetts law.[83] The Attorney General noted that users of unlicensed software gain an unfair advantage over businesses that follow the rules.[84]

In addition to its fine, Narong has agreed not to illegally use unlicensed copyrighted software to produce or manufacture goods that enter Massachusetts.[85] Narong also conducted an internal audit of its IT system to ensure compliance with IP law. It is not clear whether it did so at its own initiative or under the terms of its agreement with the Massachusetts AG. The enforcement was reportedly supported by some in the local business community, who cited the harms done to local employment.[86] Unions were reportedly also supportive of the Attorney General's action, including the American Federation of Labor and Congress of Industrial Organizations ("AFL-CIO").[87] Lawyers in Thailand are warning local companies with business in the United States to tread carefully in this area.[88]

California undertook a similar action in January 2013. The state Attorney-General filed lawsuits in Los Angeles County Superior Court against two companies for their use of pirated software in the production of apparel imported into and sold in the state.[89] The state alleged that Ningbo Beyond Home Textile Co., Ltd., a Chinese company, and its affiliates, and Pratibha Syntex Ltd., an Indian company, installed and used software without paying the licensing fees.[90] This in turn allegedly gave the Chinese and Indian companies a "substantial and unfair" cost advantage over their license-paying competitors in California. The suits also alleged that non-payment discouraged innovation, as American software companies would be discouraged from developing software given the lowered returns on investment. The relief being sought includes: an injunction against continued violation of the law, an injunction preventing the distribution or receipt of the foreign companies' garments until they are in compliance with the law, provision of a certified list of all software used by the companies every six months for the next five years, appointment of a trustee (with full access to the companies' computer systems, to verify compliance, attorneys' fees, and a penalty of US$2,500 "against each Defendant for each violation" of the code.[91] The complaints did not make clear what constituted a single violation.

Although this enforcement action is against pirated IT, the Attorney-General's press release and the reasoning explained in the complaint suggest that similar action could be taken against other forms of Unauthorized IP. The Attorney-General stated that "[c]ompanies across the globe should be on notice that they will be held accountable in California for stealing our intellectual property."[92]

In addition to their scope, state UDAP statutes may differ in enforcement. All of these laws are enforced by a state governmental agency, usually the state's Attorney-General, and most but not all can also be enforced by certain private parties. A state agency could choose to act on its own or it might first be approached by a competitor or the aggrieved IP holder.

Penalties also vary by state, although all offer some form of equitable relief and/or damages. All but one state authorize the state agency to seek civil penalties for a violation of the state's UDAP statute.[93] In some instances, in addition to compensatory damages for consumers, these include multiple damages and/

80 MASS. GEN. LAWS ch. 93A, § 2 (2012). Contrary to some press reports, the law does not specifically state that businesses using unlicensed software should not gain unfair advantage over competitors who follow the law.

81 See Narong Seafood Co. Ltd., http://www.narongseafood.co.th/ (last visited July 19, 2013).

82 See, e.g., Michael B. Farrell, Massachusetts Fines Thai Seafood Company over Pirated Software, BOS. GLOBE (Oct. 19, 2012), *available at* http://bostonglobe.com/business/2012/10/18/massachusetts-fines-thai-seafood-company-over-pirated-software/ZdfHGXTTSVMzll0pQLcnhP/story.html; Ira Kantor, Thai Seafood Company to pay US$10G Penalty over Unfair Practices, BOS. HERALD (Oct. 18, 2012), *available at* http://bostonherald.com/business/technology/technology_news/2012/10/thai_seafood_company_pay_10g_penalty_over_unfair; Patricia Resende, State Fines Thai Company for Pirated Software Use, BOS. BUS. J. (Oct. 18, 2012), *available at* http://www.masshightech.com/stories/2012/10/15/daily46-State-fines-Thai-company-for-pirated-software-use.html.

83 Farrell, *supra* note 82.

84 *See* Assurance of Discontinuance pursuant to G.L. c. 93A, Sec. 5, *Comm. of Mass. v. Narong Seafood Co., Ltd., No. 12-3825A*, at ¶ 5 (Mass. Sup. Ct. Oct. 18, 2012).

85 *Id.* at ¶¶ 8-10.

86 Resende, *supra* note 82.

87 *Id.*

or punitive damages. As noted above, even where damages are assessed, the greatest risk may nonetheless be the injunctions – a ruling that a company could not import products containing components produced by a supplier using Unauthorized IP – could be very challenging (and if replicated in important and/or numerous states, potentially crippling). Most states (forty-five plus the District of Columbia) do not require the state agency to prove the business's intent or knowledge in order to impose a remedy,[94] suggesting that it may be incumbent on companies to study whether they themselves are using Unauthorized IP or whether it has been incorporated in their supply chains.

Enforcement Risk 5: Withdrawal of Suppliers

Companies also face the risk that its suppliers will stop supplying it with components. In addition to the reasons cited above – injunctions by the ITC or by individual states, for example, or determining that the risks exceed the rewards of continuing the supply relationship – a supplier might also face direct legal challenges to its use of IP that does not belong to it. Although IP litigation is beyond the scope of this White Paper, it is worth describing one recent notable case to demonstrate the punishment that can be visited companies that violate IP rights. In 2009, DuPont filed a complaint against Kolon Industries, a South Korean competitor, in connection with the latter's alleged misappropriation of DuPont's trade secrets. Following a trial, a jury found that Kolon had willfully and maliciously misappropriated DuPont's trade secrets through the use of former DuPont employees as consultants, using at least one of them to funnel stolen trade secret information to Kolon and even secretly copying that consultant's computer during a lunch break. In addition to punishing Kolon with a staggering verdict of US$919.9 million in compensatory damages, the court ultimately issued injunctions to them, prohibiting them from producing the offending product at all for the twenty years and permanently enjoining them from either using or disclosing the trade secrets that they had learned.[95]

All states – like Virginia in the *DuPont v. Kolon* case – have prohibitions on misappropriation of trade secrets. Forty-eight states and the District of Columbia have adopted statutes modeled on the Uniform Trade Secrets Act, with Massachusetts and New York addressing such conduct under their common law. A total of thirty-six states also expressly criminalize trade secret appropriation.

Thus a supplier could face trade secret litigation in any US state, and a finding that they violated such laws could permanently remove a supplier from a company's supply chain.

C. Developments in Japan and Europe

Japan

IP represents a critical asset for many Japanese companies today. Since 2002, the Japanese government has been strengthening existing protections for IP has established policies and institutional arrangements which promote and protect IP. The government encourages Japanese companies to create, manage and acquire IP strategically, provides efficient enforcement mechanisms through the courts and administrative hearing procedures, promotes harmonization with foreign systems and the training of specialists. Having said that, the Japanese government and Japanese companies have not yet developed a robust system to detect and protect supply chains from Unauthorized IP.

To date, we are not aware of any Japanese court or administrative cases which have dealt with the issue of Unauthorized IP in connection with competition law perspective. However, we believe that there may be remedies which can be pursued by an aggrieved party under existing law despite some conceptual differences with the US treatment of the issue. Current thinking by academics and practitioners is that use of Unauthorized IP is outside the scope of the Antimonopoly Act unless the use itself falls into an enumerated category of illegal conduct regulated

88 Charoen Kittikanya, *Narong Seafood Stung by Suit*, BANGKOK POST (Oct. 23, 2012), *available at* http://www.bangkokpost.com/lite/topstories/317953/narong-seafood-stung-by-suit.

89 *See* Complaint for Injunction and Civil Penalties Based on: (1) Violations of the Unfair Competition Law (Bus. & Prof. Code §§ 17200, et seq.), *California v. Ningbo Beyond Home Textile Co.*, No. BC499751 (Cal. Super. Ct. Jan. 24, 2013); Complaint for Injunction and Civil Penalties Based on: (1) Violations of the Unfair Competition Law (Bus. & Prof. Code §§ 17200, et seq.), *California v. Pratibha Syntex Ltd.*, No. BC499751 (Cal. Super. Ct. Jan. 24, 2013).

90 The software was from Microsoft, Adobe, Symantec and Corel Corporation. See Complaint at ¶¶ 38–39, *Ningbo Beyond Home Textile*, No. BC499751 (alleging illegal use of Microsoft, Adobe, Symantec and Corel software); Complaint at ¶¶ 38–39, *Pratibha Syntex*, No. BC499751 (alleging illegal use of software, including Microsoft and Adobe software).

91 Complaint at ¶¶ 54-61, *Ningbo Beyond Home Textile*, No. BC499751; Complaint at ¶¶ 55-63, *Pratibha Syntex*, No. BC499751.

92 Press Release, State of CA, Dep't of Justice, Office of the Att'y Gen. Kamala D. Harris, *Attorney General Kamala D. Harris Files Unfair Competition Lawsuits over Use of Pirated Software in Apparel Industry* (Jan. 24, 2013), http://oag.ca.gov/news/press-releases/attorney-general-kamala-d-harris-files-unfair-competition-lawsuits-over-use.

93 Carter, *supra* note 79, at 17 (citing Rhode Island as being the only state where the state agency is not authorized to seek civil penalties for a business's violation of the UDAP statute).

by the Antimonopoly Act – which it does not appear to do. Use of Unauthorized IP is instead more likely to be regulated by the Law Prohibiting Unfair Competition. Should the US FTC change its approach to this issue under Section 5 of the FTC Act, it is possible that opinion in Japan may change as well over time.

Nevertheless, the IP laws including the Patent Act, the Copyright Act and the Law Prohibiting Unfair Competition (including trade secrets) and the Customs Law prohibits imports of goods that infringe Japanese IP rights (excluding trade secrets infringement) into Japan and may be blocked at the port of entry. Violations of the Customs Law include fines and up to 30,000,000 yen and imprisonment for up to 10 years.[96]

Goods which are produced using illegally obtained trade secrets are not specifically subject to interdiction at the port of entry but under the Law Prohibiting Unfair Competition, it is possible for a victim or rights holder to obtain injunctions and damages. In addition, a violator is subject to criminal sanctions, which may include fines of up to 10,000,000 yen for individuals and 300,000,000 yen for corporations. Individuals can face imprisonment of up to 10 years.[97]

Given Japan's interest in promoting and protecting IP, it may only be a matter of time before policymakers take up this issue in a serious way and may even pursue international cooperation as cyber espionage and the protection of valuable IT come into sharper focus.

Europe

In the European Union ("EU"), legislation on intellectual property rights is only partially harmonized and thus continues to differ from one Member State to another.[98] Similarly, some legislation has been adopted harmonizing the enforcement of IPRs,[99] but actual enforcement of IPRs falls within competences of Member States. Therefore, the rights and enforcement mechanisms are for instance not exactly the same in France, Germany or the United Kingdom.

At EU level, the law on IPR infringement throughout the production chain is currently much less developed in the EU than in the US or Japan. The only explicit basis for an action against a producer marketing products entirely or partially manufactured with unauthorized software is provided in Article 7 (1) (b) of the Directive 2009/24/EC on the legal protection of computer programs. The Directive imposes on Member States an obligation to "*provide, in accordance with their national legislation, appropriate remedies against a person committing [an] act of...the possession, for commercial purposes, of a copy of a computer program knowing, or having reason to believe, that it is an infringing copy.*"[101] In other words, the use of unauthorized software for commercial purposes, such as the manufacture of goods, is prohibited under EU law. However, it remains unclear whether only the person *directly* using unauthorized software can be held liable or whether downstream users of such intermediate goods may also be held liable.

94 *Id.* (the five states that require showings of intent or knowledge are Colorado, Indiana, Nevada, North Dakota and Wyoming).

95 *See E.I. DuPont de Nemours v. Kolon Indus.*, Inc., No. 3:09-cv-00058-REP (E.D. Va. Sept. 14, 2011) (Docket No. 1514) (jury returned a verdict in favor of Dupont of US$919.9 million in compensatory damages); *E.I. DuPont de Nemours and Co. v. Kolon Indus., Inc.*, 894 F.Supp. 2d 691, 694, 721 (E.D. Va. Aug. 30, 2012) (granting DuPont's motion for an injunction against Kolon), stayed pending appeal by 2012 US App. LEXIS 20290 (4th Cir. Sept. 21, 2012).

96 Kanzei-ho [Customs Law], Law No. 61 of 1954, art. 109 (Japan).

97 Fusei Kyoso Boshi-ho [Law Prohibiting Unfair Competition], Law No. 47 of 1993, arts. 21, 22 (Japan).

98 *See generally*, Council Directive 89/104, To Approximate the Laws of the Member States Relating to Trade Marks, 1989 O.J. (L 40) 1 (EEC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1989:040:0001:0007:EN:PDF; Directive 98/71 of the European Parliament and of the Council of 13 October 1998 on the Legal Protection of Designs, 1998 O.J. (L 289) 28 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31998L0071:EN:HTML; Directive 98/44 of the European Parliament and of the Council of 6 July 1998 on the Legal Protection of Biotechnological Inventions, 1998 O.J. (L213) 13 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:1998:213:0013:0021:EN:PDF; Directive 2001/29 of the European Parliament and of the Council of 22 May 2001 on the Harmonisation of Certain Aspects of Copyright and Related Rights in the Information Society, 2001 O.J. (L 167) 10 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:167:0010:0019:EN:PDF.

99 *See generally*, Directive 2004/48 of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, 2004 O.J. (L 195) 20 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:195:0016:0025:en:PDF; Council Regulation 1383/2003, Concerning Customs Action Against Goods Suspected of Infringing Certain Intellectual Property Rights and the Measures to be Taken Against Goods Found to have Infringed Such Rights, 2003 O.J. (L 196) 7, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:196:0007:0014:EN:PDF.

100 Directive 2009/24 of the European Parliament and of the Council of 23 April 2009 on the Legal Protection of Computer Programs, 2009 O.J. (L 111) 16 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:111:0016:0022:EN:PDF.

101 *Id.* at art. 7(1).

Despite the absence of case-law specifically on point, guidance might be found in the cases in which the Court of Justice of the European Union (CJEU) discussed the concept of secondary liability for IP rights infringements in the context of protection of registered trademarks. In two recent cases related to online services, the Court held that a reference system provider and an operator of an online marketplace cannot escape liability where they knew of the infringement and did not act.[102] Although the context is different, this line of case-law in effect imposes on traders in certain circumstances a duty of care not to trade or help trading in goods infringing IPRs and stresses that third parties may be held liable for IP infringements that they had not committed themselves.

Moreover, the EU recognizes the growing importance of effective protection of intellectual property and offers a number of measures that are supposed to intensify, increase effectiveness and coordinate enforcement of IP rights. Recent Council Resolution on the EU Customs Action Plan to combat IPR infringements for the years 2013 to 2017 sets out several strategic objectives, including tackling trade of IPR infringing goods throughout the international supply chain.[103] The resolution envisages a number of mechanisms strengthening coordination with countries considered the key source of infringing products, transit and destination countries. Enhanced information exchange should allow for a close monitoring of main problems relating to IP rights infringement in all that countries and prevent targeted products from entering into the EU territory. The resolution paves the way for further actions both at EU and national levels.

At national level, Directive 2004/48/EC on the enforcement of intellectual property rights imposes on Member State a general obligation *to provide for the measures, procedures and remedies necessary to ensure the enforcement of the intellectual property rights.*[104] The scope of these rights, definition of 'infringement' and mechanisms for attributing liability differ between Member States. Therefore, possibility of commencing an action against a producer using in its production chain infringing goods, depends on the relevant national legislation. In that regard, it is interesting to note that the European Commission has launched a public consultation on the effectiveness of the remedies available at national level for the enforcement of IPRs. It will be interesting to see whether the results of the public consultation leads to the enactment of specific legislation combatting unauthorized IP use in the supply chain similar to the measures adopted by some US States.

Finally, an individual could potentially bring an action under the national unfair competition acts of the 28 Member States. As unfair competition entirely falls within the competences of the Member States, the requirements to bring an action and the available remedies differ from Member State to Member State. Although unfair competition provisions often mainly focus on advertisements and conduct that misleads consumers, they often define so broadly what constitutes unfair competition that they could arguably be relied upon to lodge an action against an importer of goods tainted by unauthorized IP use in the supply chain.

V. Other Risks: Reputational Harm & Boycotts

Finally, in addition to the legal claims discussed above, companies that use Unauthorized IP or have it in their supply chains potentially face other, non-legal risks, including harm to their reputation and possible boycotts of their products.

Both IP owners and competitors have an incentive to publicly shame companies that take advantage of Unauthorized IP, whether they are suppliers or sellers of end products. Other entities, such as business groups or even unions, can play a similar role, as we saw in the Narong Seafood case. Non-US companies would be particularly susceptible to criticism that they are flouting the law and thereby gaining an unfair advantage over law-abiding US businesses. These criticisms might play out in the form of articles by the media or even, at the extreme in product boycotts and the like. They could also lead to government enforcement action.

102 *See, e.g.*, Case C-324/09, *L'Oréal SA v. eBay I* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:195:0016:0025:en:PDF *nternational AG, 2011 O.J.* (C 269) 3.

103 *See* Council Resolution on the EU Customs Action Plan to Combat IPR Infringement for the Years 2013 to 2017, 2013 O.J. (C 80) 1, *available at* http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/intm/134125.pdf.

104 Directive 2004/48 of the European Parliament and of the Council of 29 April 2004 on the Enforcement of Intellectual Property Rights, art. 3, 2004 O.J. (L 195) 20 (EC), *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2004:195:0016:0025:en:PDF.

VI. Conclusions Concerning Supply Chain Risk

While there are only a few cases in the US that have addressed Unauthorized IP in the supply chain and none in Europe or Japan, we can nevertheless draw certain conclusions:

- The policies of the US federal and state governments, the European Union and Japan support stronger protection of intellectual property.
- The OECD studies cited above demonstrate that Unauthorized IP extracts significant value from the producers and holders of intellectual property, in addition to broader impacts on growth, criminal enterprise, the environment, employment, trade and foreign direct investment.
- The use of Unauthorized IP places companies who respect the rule of law at a competitive disadvantage when compared to those companies who do not, thereby threatening jobs and the economy in affected markets.
- In the cases cited above, the **direct** users of Unauthorized IP, either in the design, production, marketing or sales processes or as integrated into the product/component itself, have already faced or are facing legal challenges under Section 337 of the Tariff Act of 1930 and, resulting in possible limitations on their ability to import such products into US and/or related damages. Indeed, the injunctive relief may in the end be more harmful than the damages. Further, there is no intent requirement here; if a company's products are found to contain infringing IP, their import can be blocked.
- A critical question for companies selling into the United States is whether state enforcers or aggressive plaintiffs will succeed using the same legal theories under state law that have been used against direct users of Unauthorized IP, as already has taken place in Massachusetts and California. There is no clear reason why they would not, as the two cases are analogous. A state attorney general or plaintiff would argue that a manufacturer with Unauthorized IP in its supply chain gains an unfair advantage over (and harms) its competitors by using components that are cheaper by virtue of the fact that they are either comprised of Unauthorized IP or were designed, produced, marketed or sold using Unauthorized IP.
- The more direct threatening action may come at the state level, as state attorney generals, who are acutely aware of harm to local businesses and employment prospects in their respective states, follow the examples set in Massachusetts and California. As noted above, the state unfair competition and UDAP statutes discussed above are broad and many are likely to encompass the conduct at issue here.
- Another threat at the state level is from laws, like those in Washington and Louisiana, which specifically address Unauthorized IP in the supply chain (in those cases, unauthorized IT in particular).
- We believe that companies who feel under pressure because of thin margins or loss of market share are increasingly likely to begin the test the limits of the legal theories described above.
- Risk mitigation through the proven techniques we describe in the next section is a wiser and less costly option when compared to a "full throttle" attack in the US, under both federal law and numerous state laws, and can place companies out front of future developments in Europe and Japan.

VII. Risk Mitigation: How Should Companies Respond?

While the legal frameworks for protecting intellectual property across Asia are gradually improving, it is fair to say that the rule of law is not as strong as it should be and as a practical matter, there are often no viable remedies for foreign holders of intellectual property. Accordingly, industry itself must address these issues through supply chain management techniques but currently there are no internationally recognized industry standards concerning best practices in monitoring the supply chain for Unauthorized IP. It should be clear that this concern is not just a matter of better corporate citizenship but is of strategic importance to any company that wishes to ensure the sustainability of its supply chain and mitigate external threats. As the analysis above demonstrates, it is not difficult to imagine a scenario where a critical Asian supplier is financially damaged by a lawsuit for employing Unauthorized IP and is consequently unable to supply a buyer on a continuous basis.

It is incumbent on forward-looking companies to consider how to fully comply with the relevant laws, address the associated business risks, and avoid the financial damage and reputational harms associated with Unauthorized IP. This will require affirmative steps. But there is a silver lining: the costs of compliance are relatively low given the downside risks, and many of the compliance efforts that we recommend primarily require refocusing existing compliance policies. The following measures, when taken together, should help to mitigate those risks and place compliant companies in a better position to defend their procurement practices.

- Know your supply chain
- Protect yourself contractually
- Institute compliance policies and build awareness
- Publicize your policy and work with industry groups
- Take the lead in developing new standards, rules and best practices

The Emerging Risks of Unauthorized IP in Your Supply Chain and How You Should Respond

Measure One: Know your supply chain

It is incumbent on any business for them to know their supply chain. Recent disasters caused by earthquakes and tsunami in the Tohoku region of Japan and flooding in Thailand have signaled to the world that supply chain disruptions can be very damaging. Worse yet are the risks of forced or child labor or the incorporation of components that pose health or safety risks to consumers. Global companies now monitor such risks as a matter of course. Numerous consulting companies provide advice on how to uncover the hidden risks in their supply chains and make suggestions for mitigation.

Many leading international companies currently monitor their supply chains for the four UN Global Compact areas (human rights, labor, environment and anti-corruption) and require all of their suppliers and sub-contractors i) to allow access to all offices and work locations, ii) to interview supplier and subcontract personnel and iii) to make and retain copies of any records concerning compliance with contract requirements and local law. These techniques can readily be adapted to issues related to Unauthorized IP but audits alone will not solve the problem. For example, it is well-known that there are many "CR consultants" in China who are hired by factory managers to fool auditors by creating false accounting and other records. Other steps are needed. Most global companies already pay close attention to supply chain management and have already mastered many other aspects of supply chain risk mitigation.

Measure Two: Protect yourself contractually

Companies that intend to positively address this problem can provide in their contracts with suppliers representations and warranties and covenants to the effect that the products or components supplied do not and will not contain Unauthorized IP and provide for the assessment of damages or penalties in the event that the these provisions are breached. That will place the burden of this risk on the supplier and will provide the basis for terminating the relationship if there are violations. In addition, contracts with first-tier suppliers can provide that such supplier must insert similar clauses in contracts with its own sub-suppliers and so forth down the line. Such contracts might also provide for indemnification in the event that the company is sued by a US plaintiff, state attorney general or federal antitrust authority under one or more of the legal theories discussed above.

Many large brands have hundreds or even thousands of companies in their supply chains. Some of these suppliers also use third party contractor personnel. Of course, one must decide as a practical matter how this requirement can be applied far down the supply chain but in many cases, a significant amount of procurement (e.g., up 80%) may be provided by a rather concentrated number (e.g., 20%) of the suppliers. In that event, it might be practical to direct compliance efforts toward certain "focus countries" and "focus factories" that are likely to account for a large amount of Unauthorized IP. If improvements are achieved there, a manufacturer can feel more comfortable that its supply chain will not be threatened by a crippling lawsuit like the one seen in the DuPont case above.

Measure Three: Compliance training and awareness building

Global companies are now attuned to the need to comply with the law of numerous jurisdictions as they conduct business across borders. Risks related to regulatory non-compliance, money-laundering, bribery and antitrust violations are among the issues that are a top priority for many companies. They have written policies, training sessions and monitoring processes which help responsible officers implement compliance measurers because they understand that the cost of compliance (while burdensome in many instances) is still cheaper than the damage to reputation and the payment of large penalties and damages. Given the trends toward more enforcement against the use of Unauthorized IP in the supply chain as discussed above, the same can probably be said with respect to this area as well.

Compliance programs must be actually implemented in practice in order to have any real value in promoting the right type of corporate behavior but when done properly, such programs can actually educate employees, customers and suppliers. At this stage in the development of the law, it is difficult to say whether a properly designed and implemented compliance program would provide a complete or partial defense to an action based one of the theories described above but it would undoubtedly help defense arguments; particularly with respect to corporate level knowledge as to whether Unauthorized IP is being employed.

Measure Four: Publicize your policy and work with industry groups

Companies who wish to combat Unauthorized IP should publically announce their policy in regulatory filings, publications and on their websites. This will put present and future suppliers, customers, regulators and potential plaintiffs on notice that the company will exert its best reasonable efforts to properly manage its supply chain. This will also go a long way toward demonstrating corporate intent should it become subject to a lawsuit on one of the theories mentioned above.

While cooperative efforts among competitors are closely scrutinized by antitrust authorities in numerous jurisdictions and should only be undertaken with the greatest care, industry associations might adopt policy statements and codes of conduct which pledge all members to take affirmative steps to comply with all laws concerning the elimination of Unauthorized IP in their supply chains. With the adoption of appropriate safeguards such as the appropriate use of a trade association, such joint action should not be objectionable from an antitrust perspective and will create pressures on all suppliers to a particular industry to bring their practices into compliance. Some international companies are also experimenting with cross-industry collaboration as well in efforts to address supply chain risks. For example, some Asian factories supply a large number of components to numerous foreign buyers in diverse industries. As best practices in this area develop, numerous companies in various fields who maintain the same standards with respect to IP protection will incentivize the suppliers to comply in order to avoid multiple audits and conflicting requirements. Note, however, that you must be very careful when discussing standards with competitors and similarly situated customers whether it is within a trade association setting or other context, as authorities, private plaintiffs and terminated suppliers in many jurisdictions can be expected to scrutinize such cooperation for conduct that crosses into an area regulated by the antitrust laws. Careful consultation with qualified antitrust counsel is essential before proceeding in this area.

Measure Five: Take the lead in creating new standards, rules and best practices

Currently, there are no internationally recognized industry standards or best practices in monitoring the supply chain for Unauthorized IP. If you act now to propose standards, rules and best practices, you can significantly influence the competitive landscape in your favor. Such action might be taken independently, as part of a business coalition, through national governments or intergovernmental organize.

Worldwide. For Our Clients. whitecase.com

White & Case LLP
White & Case Law Offices
(Registered Association)
Marunouchi Trust Tower Main 26th Floor
1-8-3 Marunouchi
Chiyoda-ku, Tokyo 100-0005
Japan
Tel: + 81 3 6384 3300
Fax: + 81 3 3211 5252