

9-2011

Gray Market for Information Technology (IT) Products: Status, Implications, and Strategies to Address the IT Gray Market Threat

Naveen Gudigantala

Operations and Technology Management Department, Pamplin School of Business, University of Portland, gudigant@up.edu

Pelin Bicen

Marketing Department, Black School of Business, Pennsylvania State University Erie

Follow this and additional works at: <https://aisel.aisnet.org/cais>

Recommended Citation

Gudigantala, Naveen and Bicen, Pelin (2011) "Gray Market for Information Technology (IT) Products: Status, Implications, and Strategies to Address the IT Gray Market Threat," *Communications of the Association for Information Systems*: Vol. 29 , Article 10.

DOI: 10.17705/1CAIS.02910

Available at: <https://aisel.aisnet.org/cais/vol29/iss1/10>

This material is brought to you by the AIS Journals at AIS Electronic Library (AISeL). It has been accepted for inclusion in Communications of the Association for Information Systems by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

Communications of the Association for Information Systems



Gray Market for Information Technology (IT) Products: Status, Implications, and Strategies to Address the IT Gray Market Threat

Naveen Gudigantala

*Operations and Technology Management Department, Pamplin School of Business, University of Portland
gudigant@up.edu*

Pelin Bicen

Marketing Department, Black School of Business, Pennsylvania State University Erie

Abstract:

When genuine and branded Information Technology (IT) products flow through unauthorized channels, IT gray markets emerge. Gray markets for IT products represent a grave threat for many IT companies. Monetary losses in profits due to IT gray markets are estimated to be in the billions of dollars. Despite the importance of guidance in addressing the IT gray market threat, the paucity of IS research in gray markets is surprising. In this article, we discuss the IT gray market phenomenon, present the legal status of gray markets in several developed and developing nations, suggest some strategies to address the gray market problem, discuss implications, and call for future IS research in this important area.

Keywords: IT gray markets, Information Technology products, strategies to counter gray markets, legal status of gray markets

Volume 29, Article 10, pp. 185-202, September 2011

I. INTRODUCTION

In the last few years, the Information Technology (IT) industry has made headlines not only for innovative products but also for its increasing vulnerability to gray market activities. *Gray market activity* refers to the sale of genuine, branded products through distribution channels not authorized by the manufacturer or brand owner. In 2003, a Massachusetts based company called S-Systems Inc. received \$5.7 million worth of computer equipment from Compaq for \$3.1 million through a special education discount intended for universities. However, it was later discovered that S-Systems Inc. acquired the discount using a university as a front and sold the computer equipment in the gray market [HP, 2003]. Computer network giant Cisco indicated in its annual partner conference in 2007 that sales in its switch and router segments declined by 7 percent because of transactions in unauthorized channels [BizForum, 2011]. These two examples illustrate the prevalence of the gray market for IT products. In fact, the growth of gray market activity in the IT industry has been alarming. Surveys by KPMG show that the gray market activity in the IT industry has increased from \$40 billion in sales and \$5 billion in lost profits in 2002 to \$58 billion in sales and \$10 billion in lost profits in 2008 [AGMA, 2003; KPMG, 2008].

Many IT companies, including Microsoft, Apple, Intel, Cisco, and HP, have been encountering the negative consequences of gray markets. Because profits go to unauthorized channel members rather than the authorized ones in the case of gray markets, authorized channel partners suffer reduction in sales and profits, which causes disruption in manufacturer–distributor relationships. Because most gray marketers do not guarantee the kind of product warranties and customer service in the same breadth as the original manufacturer, the product reputation is at stake in the long run [Michael, 1998]. In addition, when genuine products are sold at a discounted price because of gray market activity, the esteem in which products are held by customers is reduced, causing the erosion of brand image [Myers and Griffith, 1999]. Despite being aware of the threat imposed by the gray markets, not many IT companies have been able to develop effective strategies to counter the threat [AGMA, 2008a]. As far as the authors are aware, not a single study in the Information Systems literature has examined the IT gray market phenomenon, discussed the implications for IT companies, and proposed strategies to counter the IT gray market threat. The research for this article, to our knowledge, is the first attempt to bridge this gap.

The objective of this article is to introduce the IT gray market phenomenon, discuss the current status of IT gray market and the implications for IT firms, and prescribe some strategies for addressing the IT gray market threat. The article is organized as follows. First, we discuss the phenomenon of the IT gray market, including types of gray markets, legal status of gray markets in international markets, and antecedents and consequences of IT gray markets. Second, we discuss some strategies for IT firms to address the gray market threat. Finally, we provide implications for IT companies and customers, call for future research to prevent IT gray markets, and end with conclusions.

II. GRAY MARKETS

Based on the KPMG survey, the major product segments affected by the IT gray market are computers, servers, computer memory, network products, processors, and hard-disk drives [KPMG, 2008]. Some examples of IT products traded in gray markets are provided in Table 1. Given this context, it is important for IT companies to have a deeper understanding of what gray markets are and how they develop.

Table 1: Examples of IT Products Suffering from Gray Market Activity

Company	Examples of products suffering from gray market activity
Microsoft	Software
Xerox	Toner cartridges
Intel, AMD	Processors
Apple	iPad, iPhone
HP, Oracle	Computer equipment (servers, hard drivers)
Cisco and Nortel	Network equipment
Other IT companies	Computer servers, HDD—storage, consumer electronics, memory, network products

In this section, we will provide background on (1) types of gray markets, (2) the legal status of gray markets in international markets, and (3) the antecedents and consequences of IT gray markets. It is important to note that gray

market goods are authorized for original sale, not counterfeited, pirated, or black-market merchandise. Gray marketers buy products from a seller through unauthorized means at a price less than the prevailing market price and sell it at a profit after deducting their expenses. The difference between gray market goods and counterfeit goods is that gray market goods are genuine goods delivered through unauthorized means by authorized channels, while counterfeit goods resemble genuine products in appearance or in performance but are not original.

Types of Gray Markets

Assmus and Wiese [1995] provide a clear categorization of gray market products. In their categorization, they conceptualize three types of gray markets: (1) parallel importation, (2) reimportation, and (3) lateral importation. In addition to Assmus and Wiese [1995], we rely on previous literature [Ahmadi and Yang, 2000; Michael, 1998] to present our discussion of the types of gray markets. The extended view of gray market types, how they ensue, and how they relate to each other are presented in Figure 1.

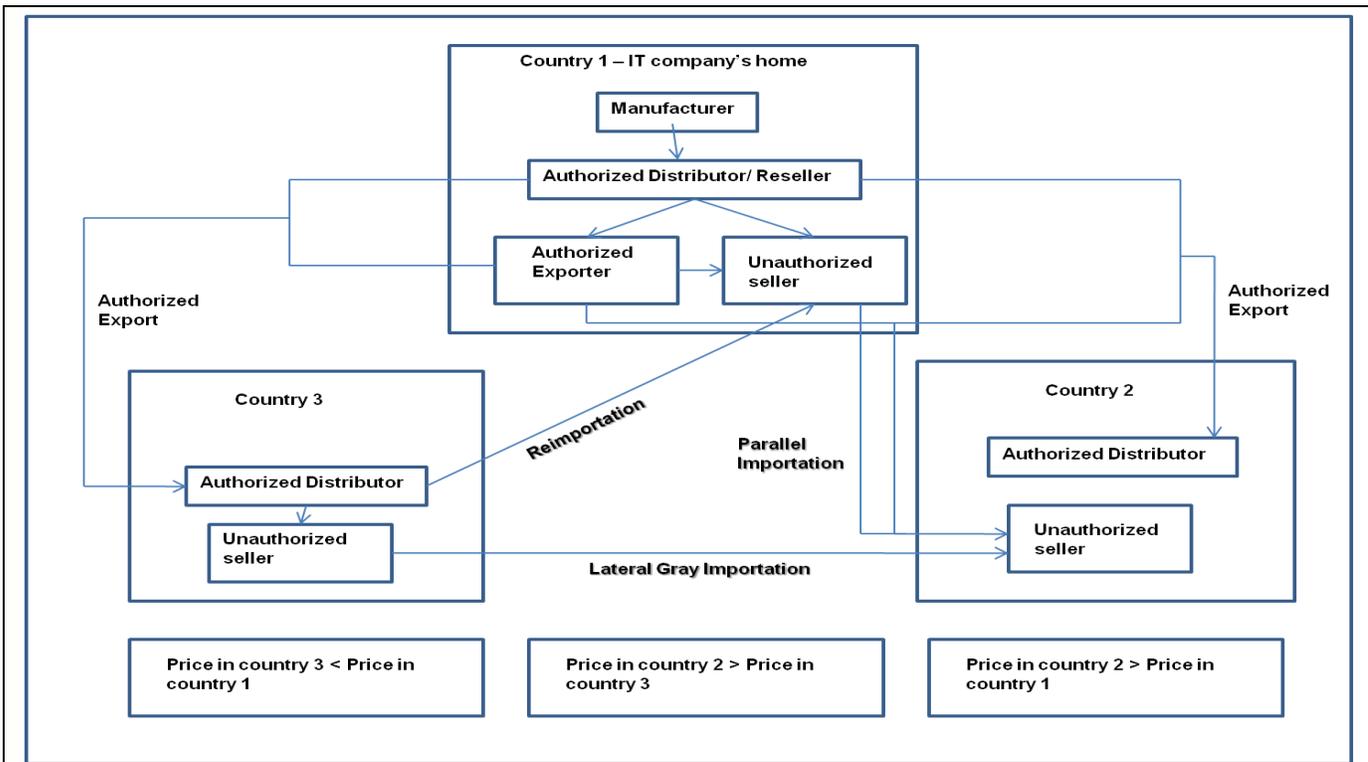


Figure 1. Types of Gray Markets

Gray markets develop in the home country of an IT company in several ways. The gray marketers purchase products at a discounted rate from any of the authorized members of the IT company's distribution channel and sell it at a profit after covering for the costs of the arbitrage. It is important to note that the authorized partners (either distributors or resellers) of the IT company, who often receive significant discounts because of promotions, are usually forbidden by their reseller contracts not to make such sales to unauthorized parties. The abuse of incentives is one of the common reasons for IT gray market goods. For instance, in 2008 HP reached a settlement with Maxicom PC Inc., one of its own sales representatives, to recover more than \$4 million offered as pricing discounts. HP alleged that Maxicom PC Inc. resorted to gray market activity by misrepresentation to resell the equipment to specific end-user customers [HP, 2008].

Reimportation occurs when products intended for a certain country resurface in the country that first manufactured and exported them. Reimportation happens because the price in the country that is supposed to receive the imports is less than the price in the country that exports them. The gray marketer can make a profit after reimporting because the cost of the arbitrage is less than the price difference. For instance, the case of Apple's Macintosh computers exported to Mexico in the mid-90s at cheaper prices relative to the prices in the U.S. market reappeared and sold in Arizona and California with English or Spanish software is an example of reimportation [Kanellos, 2006].

Parallel importation enables a gray marketer to profit when a product is priced lower in the home market than in the foreign market and the cost of arbitrage is less than price difference. In such instance, the gray marketer can parallel import the product from the country of production to the foreign market and sell it there to make a profit. For

instance, a case concerning Sun Microsystems Inc. vs. M-Tech Data Ltd. illustrates the instance of parallel imports in disk drives. Sun Microsystems Inc. was a U.S.-based company selling computer equipment. (Sun was acquired by Oracle in 2010.) M-Tech Data Ltd., an independent UK-based distributor not authorized by Sun Microsystems, purchased sixty-four Sun Microsystems disk drives from a U.S. broker, imported them into the UK, and sold them [Sayer, 2010]. It is important to note that M-Tech Data Ltd. is not on the list of the UK-based authorized resellers of Sun Microsystems. The case is now being fought by Oracle.

Lateral gray importation occurs when products from one country where the prices are lower are sold through unauthorized channels in another country where the prices are higher, and the products are not produced in either country. Prior to 2007, about 15 to 50 percent of Intel's processors available in India came from areas such as Hong Kong and Singapore [Nambiar, 2007]. This example illustrates a case of lateral gray markets in which the processors are not produced in India nor in Hong Kong or Singapore. However, the prices of Intel's processors in India used to be higher than the price in Hong Kong and Singapore, thus allowing gray marketers to profit from lateral gray importation.

The problem with IT gray market goods is that these goods compete with the legitimate channel members' goods, and while the authorized channel members typically incur promotion and advertising expenditures, gray marketers generally do not have such expenses and, therefore, benefit in an unfair manner. Overall, gray markets are detrimental to all forms of cross-border exchange and to the bottom lines of several IT multinational companies. Although gray markets may severely impact IT firms' profitability and brand reputation, the legal status of gray markets in international trade is neither clear nor uniform. In the next section, we will describe the current legal treatment of gray markets in international markets.

The Legal Status of Gray Markets in International Markets

In the broadest international legal terms, the debate over whether to allow intellectual property (IP) rights owners to control, and, hence, restrict the unauthorized imports of legitimate products, stems from the adoption of the territorial exhaustion view of IP rights. There are three doctrines regarding the territorial exhaustion view of IP rights: national exhaustion, international exhaustion, and regional exhaustion.

Under the doctrine of national exhaustion, control over distribution channels by IP rights owners is exhausted upon the first sale *within* that country. However, this does not prevent IP rights owners from fighting parallel imports in other ways. The adoption of the national exhaustion view has a strong influence on the legal status of gray markets in the United States [Maskus, 2000]. For example, the U.S. mostly embraces national exhaustion with some exceptions. However, U.S. trade laws concerning gray market are not uniform. Differences are seen among regulations regarding trademarks, copyrights, and patents. In trademark-related gray market cases, Lanham Act section 42 and Tariff Act section 526 provide protection against gray market activities. Lanham Act section 42 prohibits the importation of goods, which falsely designate origin, causing a consumer to confuse a genuine product with a gray marketed product [Swanson, 2000]. Similarly, according to the Tariff Act section 526, genuine goods are protected by the first sale doctrine and gray market activities of such goods are prohibited. However, the U.S. customs service interprets Tariff Act section 526 to permit gray market activities under three conditions. These conditions, also known as common control or affiliation exceptions, are as follows: (1) foreign and U.S. trademarks owned by the same business entity, (2) foreign and U.S. trademark owners are parent and subsidiary companies, and (3) genuine product when manufactured in a foreign factory and the U.S. trademark owner gives permission for entrance of this product into the U.S., even if it is intended for sale outside the U.S. These exceptions are designed to prevent multinational companies from engaging in monopolistic price discriminations [Lansing and Gabriella, 1993]. For copyright-related gray market cases, the main applicable regulation is the Copyright Act section 106 (3). This law's main objective is to maintain a balance between two competing policy interests—providing economic incentive to creators and providing public access to works for further development and benefit to public [Rowley, 1998]. Finally, patent laws provide patent holders exclusive rights to make, use, sell, or import a patented process and/or product [Swanson, 2000]. Patent Act section 271 protects the patentee's exclusive rights against infringement caused by gray market activities [Donnelly, 1997].

Under the doctrine of international exhaustion, IP rights are ended upon first sale everywhere in the world, and gray markets are permitted. International exhaustion is a policy generally seen in most developing nations and is favorable to the gray marketers. However, developed nations such as Australia and New Zealand have moved toward more liberal treatment of gray markets. The Australian Competition and Consumer Commission's (ACCC) study found that Australian consumers of packaged business software paid, on average, 27 percent more than U.S. consumers during the decade ending in December 1998 [Alston, 2001]. To combat the monopoly of a few IT companies and to reduce the prices of software and video games, the Australian government introduced amendments to the Copyright Act to lift restrictions on parallel imports [Alston, 2001]. In May 1998, the New Zealand government accepted international exhaustion regime for gray markets of copyrighted goods due to high prices of

compact discs and books¹ [Maskus, 2000]. Although music companies recognized that this decision will significantly impair their market segmentation and pricing policies, the New Zealand government argued that acceptance of international exhaustion in copyrighted goods will reduce the prices of consumer goods without disrupting the creative process, and thereby increase the consumer welfare in the long term. After this decision, New Zealand was included in the U.S. Special 301 watch list.²

Japan also supports the international exhaustion view of IP rights. However, different from Australia and New Zealand, the Japanese government allows contracts and notices to prevent gray market activities in their country. The implication is that the IP rights holder can prevent gray market sales by placing restrictions on the IP rights conferred through selling the genuine product. Accordingly, once the Japanese IP rights holder or related entity sells the goods outside of Japan, if explicit agreements and notices preventing the third party from distributing the goods back into Japan are not put in place, the IP rights are exhausted everywhere in the world [Swanson, 2000]. As one of the most developed nations in the world, Japan's embracing of international exhaustion of IP rights might have implications for several countries' trading relationship with Japan.

Finally, as an intermediate regime, regional exhaustion permits gray markets within a group of countries, but IP rights are not exhausted by first sale outside of the region. For example, the European Union (EU) adopts regional exhaustion in all fields of IP (e.g., copyrights, trademarks, patents) within its member countries. First sale doctrine applies within the EU, meaning that lawful sales within the EU exhaust the IP rights only within the EU, not internationally. The exhaustion of rights principle may be extended to situations where the IP owner consents to the importation and sale of the genuine product. In that case, gray market will be allowed from outside the EU. According to the Article 30 of the Treaty of Rome, free circulation of products and services should take precedence over IP rights. The basic motivation for adopting this regime was to encourage regional market integration [Li and Maskus, 2006]. The laws regarding gray markets are more developed in the EU than in any other area of the world [Donnelly, 1997].

The countries mentioned so far are mostly developed nations with established trade laws and regulations. For these, it is practical to embrace one of the three exhaustion doctrines. However, there are also developing countries whose trade regulations are still a work-in-progress. Although the analysis of every nation's treatment of the gray market activities is beyond the scope of this article, we will provide an overview of two developing nations' treatment of gray markets: Russia and China.

Russia is known to be one of the hotbeds of gray marketers. For example, in 1997 the U.S. software industry declared a loss of \$400 million because of Russian gray market [Tomlinson, 1997]. Further, in 2008, the U.S. named Russia as one of the worst offenders of its IP rights because of the increasing intensity of gray market activities in Russia and Russia's inability to protect U.S. IP rights [Sugden, 2009]. Since then, Russia made some progress by introducing IP protection laws, which enable the government to enforce IP rights and punish violators [Sugden, 2009]. Part of the motivation driving the reform comes from Russia's entry into the World Trade Organization [Portnova, 1998]. Part 1 of the Russian Civil Code deals with addressing IP rights violations. Although some progress has been made, many of these legal protections are still unclear. Therefore, IT companies planning to participate in the Russian market must be vigilant and take precautions to protect their brands.

China has limited IP rights protection and is perceived as one of the major offenders against current international IP protections [Li, 2002]. For example, a Business Software Alliance report in 2003 indicated that nine out of ten software copies sold in China during 1992 were gray market products [BSA, 2003]. The gray market for software in China is thought to result in U.S. software industry losing approximately \$2.4 billion [Li, 2002]. Microsoft is one of the major victims of the Chinese software gray market [Shen, 2005]. Unfortunately, software-related gray market activities affect global IT companies' confidence in investing their latest technologies in China and hurt the ability of the Chinese software industry to progress. According to a survey conducted by the Chinese government, the software gray market is the number-one factor impeding the progress of the Chinese software industry [Li, 2002].

In the Trade Related Aspects of Intellectual Property Rights (TRIPS) agreement of WTO, developing countries like China are given more time for IP rights implementation. The basis of this recommendation for delayed implementation seems to come from the idea that developing countries may benefit from a weaker IP regime in the period during which their economies are emerging [Maskus, 2000; Shen, 2005]. For example, a weak IP regime

¹ According to the New Zealand Institute of Economic Research [1998], the compact discs and books' prices were 20–30 percent more than U.S. prices [Maskus, 2000].

² Special 301 report examines in detail the adequacy and effectiveness of intellectual property rights in many countries around the world [U.S. Trade Representative's 2006 Special 301 Report]. Countries may be included in the categories of Priority Watch list, Watch list, and Section 306 Monitoring status based on their decision on IP rights.

embraced by U.S. in the early stages of its economic development has played a substantial role in its technology learning and accumulation. Apparently China is undergoing a similar evolution [Sugden, 2009] and beginning to take some positive steps. Currently, the IP rights protection laws, passed in the 1980s and 1990s but not implemented adequately during those times, are enforced by the Chinese government against the gray marketers. Although enforcement to protect IP rights in China is in its infancy, there is reason to be optimistic about its progress. The impending threat of sanctions by the U.S. government, an intense pressure to meet the WTO entry requirements, and, most importantly, China's own aggressive innovation strategies and globalization of their companies are the real impetus behind China's increased efforts to protect IP rights.

The disagreement on which exhaustion doctrine makes more sense in global terms stems from the Trade Related Aspects of Intellectual Property Rights (TRIPS) agreement of the World Trade Organization (WTO). When the TRIPS agreement was concluded during the Uruguay Round of negotiation of the (then) General Agreement on Tariffs and Trade (GATT) in 1994, there was clearly no consensus on the contentious issue of parallel imports. Rather, Article 6 states that, "For the purposes of dispute settlement under this Agreement, subject to the provisions of Article 3 and 4, nothing in this Agreement shall be used to address the issue of the exhaustion of intellectual property rights."³ The take away from Uruguay Round and TRIPS is that each country is responsible for establishing its own regulations for gray markets. Though TRIPS does not explicitly recognize the international exhaustion regime, it essentially allows for gray market activities to take place in the global arena. Because the issue of gray markets lacks legal clarity across the world, global IT companies are mostly on their own in countering the gray market threat. Therefore, concerned IT companies must develop and implement their own strategies to reduce the incidences of gray markets. Regulations concerning gray markets in some developed and developing countries are summarized in Table 2.

Antecedents and Consequences of IT Gray Market Activities

It is important to understand the factors that produce IT gray markets and the consequences of gray market activity for IT firms' distribution channel partners and consumers (see Figure 2). Multinational IT companies typically set different prices in different markets based on market conditions, purchasing power of consumers, and competition. Gray markets emerge when the price differential across different markets is profitable for sellers after covering for arbitrage-related expenses [Duhan and Sheffet, 1988]. Earlier examples showed that Australian consumers paid more for certain IT products than U.S. consumers, and prices for Intel's processors were higher in India during 2007 compared to the same in Hong Kong and Singapore. Differences in prices across markets provide a strong incentive for gray marketers. Within the home market of IT companies, one of the major reasons for a price differential is the incentive abuse by distribution channel partners. It is a common practice for IT companies to provide various kinds of discounts to channel partners such as contractual discounts, channel partner accreditation discount, programmatic discount, end user discount, etc. These discounts can sometimes amount to 55 percent on the list price [Deloitte, 2010]. When these products are diverted into gray markets, the unauthorized parties sell the same products for as much as 20 percent less than the prevailing market prices [KPMG, 2008]. In such situations, it is harder for authorized sellers to compete with the gray markets.

Second, not all multinational companies release their product in all the markets at the same time. The time lag between product releases in two different markets provides an opportunity for the gray marketers to profit. The Amazon Kindle, though officially not released in China, was selling in Beijing's gray market for \$630, well above the \$489 that it costs in the U.S. [Fletcher, 2010]. In another instance, Apple's iPad 2 was released in the U.S. on March 11, 2011, whereas, in several other countries and Hong Kong, it was released on March 28, 2011. The time lag of two weeks proved to be a boon for gray marketers who sold the iPad2 16GB version for as much as \$1025, which is more than twice the actual price of \$499 [Elmer-DeWitt, 2011]. Finally, currency exchange fluctuations and regulatory policies have been shown to create favorable conditions for gray market activity [Assmus and Wiese, 1995].

Gray markets negatively impact IT companies, distribution channel partners, and customers. Both IT companies and distribution channel partners suffer the losses resulting out of reduced profits and sales. The KPMG survey found that 51 percent of distributors think that their competitive position will improve if the IT gray market activity is eliminated [AGMA, 2008b]. In addition, because unauthorized imports are sometimes not made to withstand the imported markets' specifications, brand reputation is likely to suffer in the long run [Myers, 1999]. Because the gray market activity erodes the profit margins of the authorized distributors, tensions are likely to disrupt the relationships between manufacturers and distributors [Assmus and Wiese, 1995]. For instance, one of Intel's regional distributors left voluntarily in 2003 blaming Intel's pricing restrictions hurt its ability to compete with the gray market [Moltzen,

³ Agreement on Trade-Related Aspects of Intellectual Property Rights, Annex 1-C, 33 I.L.M. at 1196, Article 6.



Table 2: Regulations Concerning Gray Markets in Some Developed and Developing Countries		
Country	Regulations on gray markets	Implications of regulations on gray market practices
United States	Lanham Act section 42; Tariff Act section 526; Copyright Act section 106(3); Patent Law section 271	The trade laws regarding gray market cases are not uniform. Differences are seen among trademarks, copyrights, and patents. These laws generally embrace the national exhaustion principle; however, exceptions may apply under certain conditions.
European Union	Article 30 of the Treaty of Rome	Regional exhaustion principle applies in gray market cases. First sale doctrine applies within the EU and exhausts IP rights only within the European Union. Since the EU was formed with the goal of a single market, free flow of goods is not restricted by any EU member nation. But they strictly prohibit the gray market goods flow from the international markets.
Australia	Copyright Act; Trademark Act; Patent Act	Gray market activities of copyrighted goods are allowed without the consent of the IP rights holder, whereas the Trademark Act generally permits gray market activities upon authorized affixation of the Australian trademark. Regarding patent laws, the exhaustion doctrine depends on the circumstances of the case [Swanson, 2000].
China	Trademark Act; Article 11 and 62 of Patent Act; Copyright Act	These IP related laws were passed in the 1980s and 1990s, but they were not implemented and enforced adequately during those times. Increasing tension caused by the necessity to meet the stringent WTO entry requirements, threat of sanctions by the U.S., and the growth of Chinese global businesses motivated the Chinese government to act on these laws in the 2000s. China seems to support the international exhaustion of IP rights.
Russia	Part 1 of Russian Civil Code	Part 1 of the Russian Civil Code broadly addresses the Russian IP regulations. However, since these regulations are still in progress, IP rights and their protections are still not clear.
Japan	Patent Act; Trademark Act; Copyright Act	Japan favors the international exhaustion view of IP rights. However, exceptions may apply. Accordingly, IP rights holders may prevent gray market activities through contracts and notices. The IP rights holder may prevent the channel partner from gray market activities through contracts. That means channel partners cannot resell the goods in Japan. Again, IP right holders may prevent third parties from gray market activities through placing notice of the agreement of genuine goods.

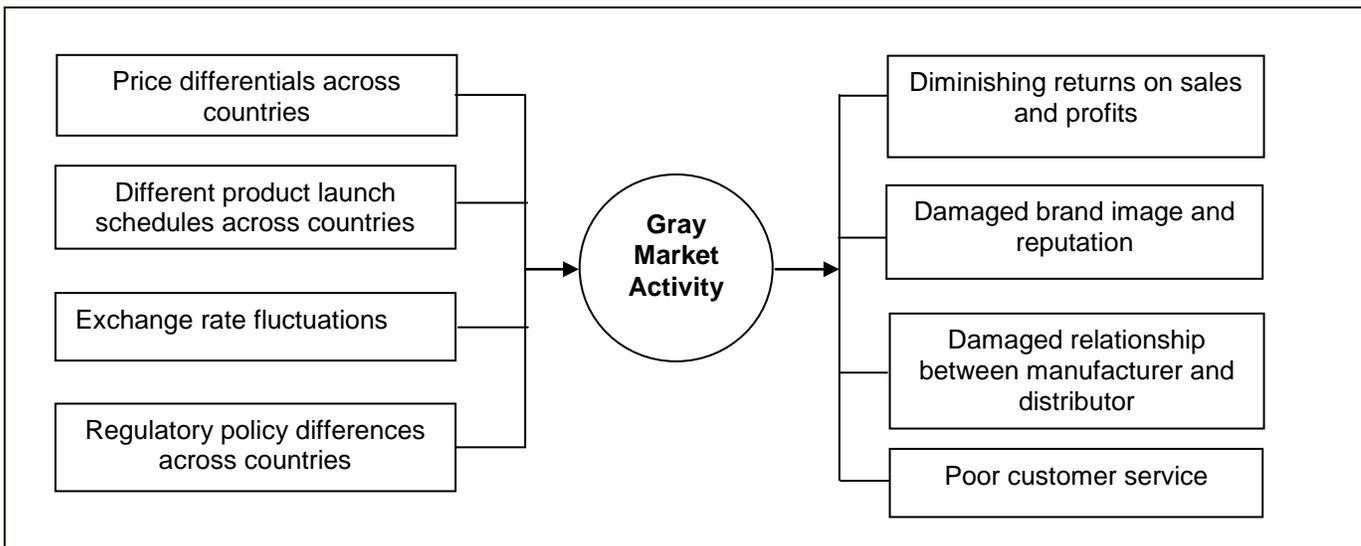


Figure 2. Antecedents and Consequences of IT Gray Market Activities

2003]. Importantly, often consumers become victims of the gray market activity. Even though there is a perception that gray market goods are cheaper; alarmingly, an estimated 60 percent of end-users in the U.S. IT market pay the same price for gray market products as they do for products sold in the authorized distribution channels [AGMA, 2003]. The customers unwittingly buy products that are delivered through gray market only to find the goods to be damaged, expired, or without customer service or warranty. These instances hurt the reputation of the brand as customers tend to blame the manufacturer for their plight.

This section has discussed the types of gray markets, legal status of gray markets in international markets, and the antecedents and consequences of gray market activities. To develop effective strategies to counter gray markets, IT managers must understand how gray markets originate, the different types of gray markets, the legal status of gray markets, and the consequences to the stakeholders because of gray market activities. In addition, the development of strategies to counter the gray market threat requires an understanding of the interconnections among different elements that give rise to the formation of gray markets and the consequences to stakeholders.

Despite the negative effects of gray market activity, the KPMG survey indicated that 42 percent of Original Equipment Manufacturers (OEMs)⁴ do not have a process in place to counter the gray market threat [AGMA, 2008b]. We suspect that the reasons for so many OEMs turning a blind eye on gray markets are multifold. It is possible that some IT companies perceive that IT gray markets provide benefits under certain circumstances. We summarize them in six parts:

1. *To increase market share:* IT companies may benefit from gray market activities when authorized products are sold in the untapped markets where there is no direct competition with authorized dealers. In another scenario, it may be possible that IT companies, despite being aware of certain markets, are not willing to enter them because of some risks. Therefore, IT companies may hedge their investments in financial and personal resources in such markets by allowing the gray markets to operate [Sugden, 2009].
2. *To overcome international regulations:* Gray markets may be beneficial if they provide IT companies to overcome any barriers imposed by foreign governments [Antia et al., 2004]. For example, China requires multinational companies (MNCs) to partner with local companies to have facilities in China. Many MNCs can take advantage of gray market suppliers in China to overcome this market entry restriction.
3. *To remain competitive in highly intensive markets:* IT industry is one of the most exploited industries by the gray marketers. According to the KPMG research report in 2003, HP, Cisco, and Intel are some of the companies whose products are actively sold in the gray markets. The report also indicates that instead of fighting back, these companies take a blind eye toward gray market activities. This way, they can match the low prices and, therefore, can compete aggressively to maintain their leadership positions in markets with intense competition. However, we believe that the situation has changed drastically since 2003, and the aforementioned companies seem to take an aggressive approach to fight IT gray markets.
4. *The cost involved in channel management:* Many IT companies may tolerate gray market activities because letting it slide may be less costly than shutting down the gray markets. Indeed, monitoring, tracking, investigating, and litigating gray market activities are expensive. Therefore, IT companies may choose to be inactive rather than initiate action against gray marketers.
5. *To provide flexibility to ever-changing market conditions:* Being flexible to changing market conditions is a “must” to IT companies to survive in competitive markets. However, because building and maintaining a supply chain takes significant amount of time, it may be hard for supply-chain partners to adapt to immediate changes. In that case, gray markets may provide flexibility to IT companies and their partners to overcome this resistance [Beth et al., 2003].
6. *To overcome supply-chain constraints:* IT companies may also allow gray markets to manage any possible shortfalls or surpluses in inventories. In other words, if channel members may need to make room for the upcoming new products by clearing the excess inventory or may be in an immediate need for certain products, the gray markets can serve as a viable option [Sugden, 2009].

Although these outcomes may be perceived as positive in the short term, gray market activities pose a formidable threat for IT companies in the long term. Therefore, it is our belief that developing and implementing effective strategies to counter the gray market threat has to be an important priority for many IT companies. The following section discusses some strategies to address the IT gray market threat.

⁴ The term *OEM* refers to Original Equipment Manufacturer. OEMs in IT context refer to companies that make products for other companies to rebrand and sell. Examples of OEMs include Intel, Dell, and HP.

III. STRATEGIES TO COUNTER THE IT GRAY MARKET THREAT

In the following section, we discuss three main strategies to address the IT gray market threat such as policy setting and enforcement, monitoring, and channel partner management. It is important to note that these strategies are neither mutually exclusive nor collectively exhaustive. We also present a discussion of some IT systems that have been proven to be useful in countering IT gray markets.

Policy Setting and Enforcement

A comprehensive policy outlining compliance and reporting requirements is important to address the IT gray market activity. The part of the provisions addressing gray markets typically includes restrictions concerning sourcing products from or to unauthorized channels, sanctions for selling to gray markets, end-user reporting requirements, incentive abuse, etc. Approximately half of the 90 OEMs responded in the KPMG survey reported that provisions concerning gray markets are missing in their reseller agreements and channel partner agreements [KPMG, 2008]. Even among the companies that contain provisions concerning gray markets, communications pertaining to provisions are transmitted through their Web-managed portals, websites, or emails, which typically lack a signed acknowledgment [KPMG, 2008].

Therefore, the first step that IT companies must consider is to modify their channel policies to include contractual provisions concerning compliance terms and conditions, reporting requirements, and sanctions for participating in gray market activities. Second, the IT companies must clearly communicate the policy to channel partners and get their signed acknowledgement. A good example of setting clear policy concerning gray market can be seen from Nortel network's reseller agreement. A part of Nortel's reseller agreement is titled "Gray market agreement," and it specifies that the "reseller agrees that they will not purchase any Nortel products from any source other than Nortel or a Nortel channel authorized to distribute the Nortel product to be purchased; or, sell any Nortel product to any party not expressly authorized by Nortel." The other parts of this gray market agreement concern a nondisclosure agreement, end-user information reporting at the point of purchase, and provisions concerning trademark use [Nortel, 2011a].

As a critical aspect of an effective compliance policy, firms must establish the right degree of punishment [Antia et al., 2004; Antia et al. 2006]. For instance, both HP [HP, 2008] and Cisco [Wright, 2007] clearly address the issues associated with gray market activity on their websites; thus, they provide a strong signal to their channel members against indulging in any such unethical practices. In addition, IT companies must follow up on their terms of enforcement and punish the violators. In 2007, Microsoft sued several companies in the U.S. for importing low-cost, educational versions of its products from Jordan and reselling them in the U.S. at regular commercial prices. One of the companies settled with Microsoft by paying \$1 million. In this case, Microsoft worked with the Jordanian government to unearth the gray market activity [McDougall, 2007]. Similarly, HP recovered more than \$1.8 million as part of its civil gray market lawsuit against S-systems Inc. In another instance, HP's compliance team worked with the Chinese authorities to stop the flow of \$1.2 million worth of HP products into the gray market [Singer, 2003].

Monitoring

Effective monitoring (also called sensing) contributes to controlling and identifying the IT gray market activity. There are three parts to effective monitoring: incentive management, internal controls, and authentication management.

Incentive Management

According to a Deloitte-AGMA survey, incentive abuse costs high-technology companies an estimated \$1.4 billion annually [Deloitte, 2010]. A significant 84 percent of the respondents of this survey believe that incentive abuse is one of the main reasons for the gray market in IT goods and estimate that about five to 10 percent of the incentivized IT products are diverted to unauthorized parties. KPMG survey indicates that 90 percent of OEMs offer incentives and 48 percent of OEMs do not verify end users when processing relevant rebates. Even for those OEMs that monitor incentives, 81 percent of the monitoring tools used by OEMs involve manual Excel-based tools. In addition, 50 percent of the OEMs do not require channel members to track serial numbers tied to the incentives [KPMG, 2008].

The results of these surveys suggest the need for IT companies to control and manage their incentive programs. One of the effective ways to prevent incentive abuse is to tie the product serial numbers to incentives and track the flow of IT products through the distribution channel by requiring channel partners to report serial numbers in their sales reporting. However, to implement this measure effectively, IT companies must place serial numbers on all products sold, including sub-components, maintain records of serial numbers and part numbers, keep the serial number database confidential, and require channel partners to include serial numbers in their sales reporting [Deloitte, 2010]. However, as the results of KPMG survey indicate, a majority of IT companies use manual-based Excel tools to manage incentive validation. To do a better job, IT systems capable of automatically reconciling

incentive claims to terms and conditions, testing authenticity of incentive use for each sale, and tracking noncompliance cases should be developed and used [Deloitte, 2010].

Internal Controls

IT companies can improve internal controls to address the gray market threat in two ways: training employees and creating a brand protection group. One of the important resources in countering the gray market threat is the employees of the IT company who work in the sales and distribution channel management and customer service [AGMA, 2008a], and yet 62 percent of OEMs do not provide formal training to educate employees or develop an internal employee code of conduct to address the gray market threat [KPMG, 2008]. It is highly recommended that key employees who interact with channel partners and end customers are identified, trained in distribution channel structures and reseller agreements, and incentivized for their efforts to identify the gray market activity. Indeed, service and warranty personnel must be educated on what to look for in substandard IT products (e.g., multiple claims on the same serial number) [AGMA, 2007].

Fighting IT gray markets is a tough challenge that not only requires top management support but also coordination among several business functions. Despite this need for cross-functional collaboration, a majority of OEMs report that they delegate monitoring gray market activity to individual business functions such as sales, marketing, and supply chain [KPMG, 2008]. IT companies need to formulate brand protection teams to address the gray market threat. Such teams typically work exclusively on fighting IT gray market issues (and issues surrounding IT counterfeit goods) using a cross-functional approach with the support of the top management. For instance, companies such as Cisco and Xerox have created brand protection teams that work exclusively on protecting the intellectual property rights of their companies, including fighting against the gray markets [Aitoro, 2007; AGMA, 2007].

Authentication Management

One of the problems limiting the capability of channel members and end customers in addressing the IT gray market is the inability to authenticate genuine IT goods and authorized channel partners. In this context, it is important for IT companies to improve the awareness levels of their customers concerning gray markets and to take measures to help concerned parties in identifying the authenticity of a product and channel partner.

For instance, Microsoft's Windows Genuine Advantage (WGA) program helps concerned parties establish the authenticity of Microsoft products through their website www.howtotell.com, which also offers important information to their customers and partners [Microsoft, 2011]. In another example, Nortel Networks helps customers search for authorized dealers of Nortel's products on their website [Nortel, 2011c]. In addition, companies such as 3Com, AMD, Microsoft, and Intel use holograms to establish the authenticity of their products. In addition, serial numbers also provide a way to check for the authenticity of the products. However, it is important for an end customer to purchase not only an authentic IT product but also to do it from an authorized dealer in order to receive the full spectrum of warranties and service provisions.

Creating awareness levels among channel partners and customers concerning gray market is very important. For instance, Nortel provides communication on their website for end users titled "Buyer Beware," which elaborately explains how end users can protect themselves from becoming unwitting victims of purchasing Nortel's gray market products [Nortel, 2011b]. According to Canon India's senior vice-president, 20 percent of cartridge market in India prior to 2008 was occupied by parallel importers. However, due to programs initiated by many Indian IT companies to educate channel partners about the pitfalls of gray markets, coupled with a measure to restructure pricing patterns, the gray market for IT products in India was reported to decline by up to 20 percent in 2008 [Economic Times, 2008].

Channel Partner Management

Channel partners are extremely valuable to many IT companies, as more than 75 percent of the revenues are generated through these channel partners [Deloitte, 2010]. For example, 67 percent of respondents of Deloitte-AGMA study reported using more than 5,000 channel partners to distribute their products into the market [Deloitte, 2010]. However, a majority of the times IT gray markets are created because of the unauthorized sales by some unethical channel partners. Successful management of channel partners is one of the most important strategies to address the gray market threat, and yet very few IT companies seem to pull it off successfully. For instance, the HP America's partner conference in 2006 proved to be a battleground for channel partners and HP to exchange jabs directed at each other concerning the gray market for HP's products [Zarley, 2006]. IT companies must be proactive in order to deny the entry of unscrupulous parties into their distribution channel and remain vigilant to identify incidences of gray market transactions. Additionally, IT companies must incentivize channel partners who have prolonged records of honoring reseller agreements and who remain committed to fair business practices. We recommend the following steps as important in channel partner management.

Proactive Check on Prospective Channel Members

Designing a distribution channel has long been recognized as an important aspect of channel management [Rosenbloom and Anderson, 1985]. IT companies usually design a distribution channel, which includes distributors, value-added resellers, and/or retailers, and include only those who meet the selection criteria [Rosenbloom and Anderson, 1985]. In this regard, performing a review of potential channel members seeking to enter the manufacturer's distribution channel represents a proactive step to minimize the gray market threat [AGMA, 2008a]. A thorough background check of the prospective distributors and resellers to ascertain whether or not they are legal entities not involved in any civil or criminal cases is recommended (e.g., UCC filings, civil litigation check, corporate status and business license verification). This act of performing due diligence proactively prepares IT companies to reduce the possibility of unethical distributors and resellers entering the distribution channel.

Periodic Audits of Channel Members

Accurate and timely information is essential in preventing gray market activities. It is important for IT companies to be constantly informed about the channel dynamics of gray markets for their goods. Therefore, verifying the exact boundaries of channel members' operation may require the concerned IT companies making on-site visits to the distributor sites. Auditing of channel members represents a control mechanism by the manufacturer to thwart any potential gray market activity. The audit not only identifies channel partners who engage in gray market activity, but also raises flags concerning potential channel members' likelihood of engaging in such activity. Therefore, we recommend that IT companies undertake periodic unannounced audits to identify any gray market activity in the distribution channel. By incorporating a mechanism of incentives for honest channel members and punishments for violating members, audits are likely to discourage sellers from indulging in gray market activities. For instance, HP CEO (in 2005) Mark Hurd said, "the thesis is that all partners are not necessarily equal ... not to be negative, but we have some partners that don't always do exactly what we like" [Burke, 2005]. He added that some partners are investing their hard-earned money to distribute bona fide HP products into the market, and HP wants to incentivize that type of behavior [Burke, 2005].

In addition, it is important to monitor the channel partner behavior for unexpected sales spikes and suspicious orders and to use automatic alerts. For instance, Briscoe, who works at HP, said, "we monitor the marketplace through various techniques. Investigating fraud and discount abuse and enhancing controls are also checks that we have in place. We'll go back and take into account our processes because the scans that are out there are always changing. HP especially keeps a careful eye on any quick sales and special pricing circulating the marketplace" [Singer, 2005].

Information Technology Systems to Help with Gray Market Prevention

IT systems are recommended in order to address gray market activity in a number of areas, including managing channel incentives, tracking product flow in the distribution channel, gathering market place intelligence concerning prices and sales spikes, and monitoring the Internet. IT companies can either develop their own systems or they can use third-party software to monitor the IT gray market activity. There are several third-party vendors such as Opsec Security, Mark Monitor, and New Momentum which provide brand protection IT solutions that have been shown to be effective in providing IT companies with the information to fight gray markets.

For instance, Epson, a worldwide leader in digital imaging products and technologies, used Mark Monitor, a California-based IT vendor, to monitor the gray market for Epson products. The use of the IT systems is reported to have an effect as the number of e-commerce websites and illegal auction websites carrying Epson gray market goods has reported to be fallen significantly between 2004 and 2008 [Mark Monitor, 2011]. Xerox is reported to be using IT tools such as GenuNet by Opsec Security to monitor the Internet for auction sites, e-mail-based forums, trade boards, B2B and B2C websites, and chat rooms to detect gray market activity. In addition, Xerox has implemented a tool called *TraceGuard Checkpoint* to track customer-level diversion and reseller-level diversion to monitor gray market activity [AGMA, 2007]. As these examples illustrate, the use of IT systems is an important approach to detect the IT gray market activity and, therefore, is recommended to be used by the IT companies. Following is a case study of how Xerox detected and implemented measures to address gray market activity.

Dealing with Gray Markets: Xerox Case Study

Xerox is a Connecticut-based multinational company with more than \$16 billion in revenue and operating with 53,000 employees around the world. Xerox has been facing a gray market problem in which primarily supplies like toner cartridges were being diverted from the authorized distribution channels. Xerox discovered the existence of gray market in 2006 when some manually marked goods prior to shipment started appearing in non-authorized geographies. The gray market activity has resulted in Xerox experiencing damaged channel relationships, dissatisfied customers and partners, and reduced revenue and profit.

Xerox first scoped the problem by understanding the causes of the gray market activity. Factors such as pricing strategies, inconsistent go-to market decisions, currency fluctuation, inaccurate demand forecasting, ineffective monitoring of product flow, etc. have been determined as the enablers of Xerox's gray market.

Using measures such as comparing orders by geography with actual usage, revenue to expected revenue at price guidelines, and achieved versus expected gross margin, Xerox determined that the losses in revenue from gray market activity were in several million dollars.

Xerox' brand protection group started working together with other departments such as product development, manufacturing, supply chain, sales, marketing, legal, and finance functions to create a series of steps, which consisted of harmonizing prices across different geographical regions, developing and supporting regionalized products, and employing shipment controls. The tools employed by Xerox track gray market products, gather market place intelligence, and conduct external audits. Xerox used third-party software to monitor Internet for real-time analysis, employed authentication labels to validate genuine products, and used third-party software to track its products in the distribution channel.

As for the return on investment, Xerox began to observe the changes in unauthorized reseller availability, normalization of prices in some unauthorized channels, and improving trends in revenue. Xerox learned that achieving consensus concerning measures to control gray market will rarely have 100 percent agreement, but it is important for the top management to identify the problem and support actions taken to control gray markets. Xerox also learned that constant efforts are required to improve the monitoring process, to measure the extent of gray market activity, and to refine the toolset required to counter the gray market threat.

Source: Elizabeth Barrese, Xerox—AGMA Webinar on Best practices to combat gray markets [AGMA, 2007].

IV. IMPLICATIONS

In this section, we consider several implications to IT companies and customers concerning gray markets. First, we address the issue of gray markets in hardware versus software. Gray market for a hardware product is created when the product is diverted from authorized distribution channels. However, it is also possible for an unauthorized channel member to configure IT products with gray market components. For instance, a PC may be configured to include gray market components such as processors or hard drives. While the PC may seem completely authentic from the outside, the problem concerning gray market can be detected only when a customer encounters performance issues and sends back the PC for service to the manufacturer. The following example illustrates a case of gray market for hardware components. Chip manufacturer Intel realized that the processors sold in bulk to the OEMs for pre-built systems started appearing in gray markets during the Pentium III era. To counter this practice, Intel started selling processors directly to retail stores such as Best Buy and Fry's in clearly marked individual boxes which typically carried a three-year warranty directly from Intel. For OEMs, Intel provided processors not in retail boxes, but in trays. The OEM processors are called tray processors and the retail processors are called boxed processors. This practice, to a large extent, countered the gray market for Intel's processors [Singer, 2005]. Unfortunately, from a customer's perspective, one needs to be vigilant concerning not only gray market goods, but also counterfeit goods, refurbished goods, and second-hand goods sold as genuine goods.

Software, when compared to hardware, is relatively difficult to tamper with internally. Gray market for software is created when the software is diverted from the distribution channels without the authorization of the original software developer and sold at a cheaper price. However, software industry suffers from another serious problem called *piracy*, the treatment of which falls outside the scope of this work.

Second, we address the implications for IT companies in dealing with violating vendors. The IT companies when detecting gray market incidences can respond with a variety of penalties. These penalties range from terminating the contracts, suing the distribution channel partners, extracting the amount of discounts or rebates originally offered, and using the justice system to punish the violators. For instance, IBM punishes the violating distribution channel partners by terminating the channel partner agreement [Bannister, 1985]. In another instance, a distribution channel partner who defrauded Cisco to the tune of \$15.4 million by falsely obtaining parts and selling them in gray market was sentenced to four years in prison [AGMA, 2011]. In one more instance, Microsoft sued a Montana-based vendor who sold gray market Microsoft software, but settled out of court for \$1 million [McDougall, 2007]. However, as we mentioned earlier, it is important for IT companies to educate the channel partners about the pitfalls of indulging in gray market activities and show a strong commitment to channel partners by building strong relationships. The severity of enforcement, while certainly a required measure, should be coupled with clear policy setting and a strong commitment to work with channel members in dealing with the competitive pricing environment. In addition, prior research points to combining the severity of enforcement behavior with certainty and speed of enforcement to effectively counter the gray market behavior [Antia et al., 2006]. We believe that a combination of all the preceding measures is required to successfully address the gray market threat.

Third, we discuss implications for customers of gray market IT products. The customers can be either individuals or business enterprises. The major risks for customers of gray market IT products can be financial- or performance-related. Performance-related risk means that the gray market IT product's performance could be lower than what was promised. Financial risk means that, in case of a service or repair of the gray market IT product, the original brand owner may refuse to honor the warranty and the customer has to find a third-party source to get the product repaired and in the process incur additional expenses. On the other hand, most customers when learning about the brand owner's refusal to honor the warranty owing to gray market purchase, tend to blame the brand owner and not the unauthorized seller who originally sold the product. Some IT companies, fearing the potential damage to brand reputation, extend warranty to gray market goods and thereby add additional costs to their operations [Deloitte, 2010]. The following two real-life examples from Nortel's website illustrate the problems faced by end customers when buying IT products from gray market.

Customer bought new CallPilot server on EBAY and upgraded to latest software release. The server went down with a bug check error. Customer called Nortel Networks to complain. Investigation documented that this server had an unsupported third NIC card in the system, the MPB board was in the wrong slot, an unsupported third party hard drive had been installed and the binding orders on the NIC cards were incorrect [Nortel, 2011a, p. 3].

Another customer bought some drives from the gray market. The products failed upon installation. The customer contacted Nortel Networks to investigate. Results of the investigation showed that products were used, had been modified, and the product release listed on the product labels indicated a release that was not yet generally available. Since the customer needed the product urgently, replacements were purchased from an authorized reseller in the region [Nortel, 2011a, p. 3].

The next example illustrates another instance of gray market in computer video games. Steam is an online video game platform developed by Valve Corporation. Steam has more than 3000 games and 30 million active user accounts [Valve, 2011]. Users can purchase computer video games online, and the video game software will be associated with the user's account in such a way that users can download Steam's client and play the games from anywhere on the Internet. For users who purchase the gaming software from the open market, Steam allows them to use the online play feature by simply requiring them to register a valid CD key with a user account. However, some of Valve's video games, such as Orange Box, are priced differently in different parts of the world. Some North American users purchased inexpensive version of gray market video games from Asian sellers and tried to register the CD key with Valve. Recognizing the existence of gray market, Steam refused to let users register the gray market software, citing that a regionally restricted copy cannot be used in a different region and instead asked users to contact the sellers for a refund [Caron, 2007; Steam, 2011].

What do customers lose by purchasing IT products from gray marketers? A majority of IT brand owners invest substantially to train their authorized channel members to handle any quality related issues with their products. Only authorized channel members provide customers with genuine IT products that are supported through warranty. When customers buy from unauthorized channels, they risk the possibility of not getting support from the brand owner. In some instances, the gray marketers promise to provide warranty and service, but those claims usually fall short of the expectations. In the case of software, the licenses can be granted only by the authorized channel partners. When customers buy from unauthorized sellers, the software licenses become invalid, making the customers responsible for intellectual property rights infringement.

International customers suffer from problems similar to those mentioned above. In fact, our investigation of many IT product discussion forums revealed that a number of international customers buying gray market products do not get support from their local authorized channel partners of the brand owner. For instance, a customer in Saudi Arabia complained about not getting support for a very popular laptop from a local authorized dealer because the laptop was a gray market product purchased from an unauthorized seller [Apple Support Communities, 2011].

Despite considerable risks, why do customers buy gray market IT products? We believe that the primary reason is price. It is not uncommon for potential customers to go online and visit websites such as pricegrabber.com and dealtime.com to search for deals. Often, customers decide to purchase IT products from sellers whose prices are substantially lower than those of other sellers. Usually, significantly lower prices should signal a problem, but most customers tend to look for deals on the Internet and, in the process sometimes become unwitting buyers of gray market products. Second, most resellers need to procure IT products within a specific time period to honor their sales commitments. Sometimes gray marketers can provide products to these resellers faster than the authorized channel members. Two-thirds of channel partners in the KPMG survey indicated that products purchased from gray market are delivered within a week [KPMG, 2008]. From the buyer's perspective, price and availability seem to be the main drivers of gray market activity for IT goods.

What can customers do to avoid purchasing gray market IT goods? We believe that the awareness concerning what constitutes a gray market IT product and the risks involved in buying a gray market IT product is important. For the customers who intend to avoid purchasing gray market IT goods, we offer the following suggestions [Kessler, 2006].

1. Customers should purchase products from reputable sellers. In the case of online sellers, customers should check if the seller is registered with the Better Business Bureau. Sometimes the brand owner of the IT product provides information concerning the authorized distribution channel members on their website. Therefore, the first question customers must address concerns the authorization and reputation of the seller.
2. Customers must be aware of the price range for an IT product. If an IT product is substantially lower than what is being offered at most stores, one must suspect the offer.
3. In the case of a suspicious offer, it is important for customers to contact the seller/online merchant to ask questions about (1) the warranty coverage with the brand owner in the customer's geographic region, (2) if the product comes with accessories that work within the geographic region, and (3) the serial numbers. The serial numbers can be used to check for the authenticity of the product directly from the brand owner. Additionally, if a seller offers their own warranty coverage instead of the brand owner's warranty, the customer must ask questions about gray market. It is also not uncommon for gray market IT products to have photocopied operating manuals in languages other than the local language and to contain phrases like direct import, or imported product, etc. Therefore, customers must inspect the goods upon arrival and any suspected gray market IT goods should be promptly returned. In this respect, it is advisable for buyers to use their credit cards, as most credit cards use some sort of protection in the case of fraud.

V. DIRECTIONS FOR FUTURE RESEARCH

The issues concerning gray markets have been the subject of research in many disciplines including law, economics, marketing, and management. However, the Information Systems research area is yet to make meaningful contribution to the issues surrounding IT gray markets. The following represent some questions for future research from the Information Systems perspective:

- What are the most effective strategies to counter the IT gray market activity? A study comparing the effectiveness of various strategies would be helpful to IT companies.
- How to design a serial number tracking and management system to increase the visibility of the flow of goods in the distribution channels?
- What kind of channel integration problems arise when implementing the serial number tracking system in a supply chain?
- How can knowledge management systems help in countering the IT gray market threat?
- What kinds of analytical techniques are well-suited to identifying the patterns associated with the IT gray market activity?
- What are the effective algorithms for the Web-based agents to identify the IT gray market activity on the Internet?
- How should IT managers incorporate strategies into overall corporate strategy and vice versa?

These questions represent only a small number of issues that concern the IT gray market. There are several opportunities for research into IT gray market that can provide effective solutions to preventing channel incentive abuse, monitoring gray market using IT systems, and authenticating IT products in the distribution channels.

VI. CONCLUSIONS

Our main objective in the article has been to highlight the IT gray market phenomenon, explain how gray markets operate for IT products, enumerate the legal status of gray markets in some developed and developing countries, and to offer some strategies to counter the IT gray market threat. We believe that several IT companies are not well prepared to address the threat posed by the gray markets. We suspect that some might believe that gray markets may benefit them in some ways. However, as we argued in this article, the belief that gray markets are good is dangerous and in the long run, gray markets can wreck havoc in several ways.

Gray markets are becoming a serious threat to IT companies' bottom lines. The extent of losses has bothered companies such as Motorola, HP, DuPont, and 3M so much that they have employed full-time managers and staff to address the gray market threat [Antia et al., 2004]. In addition, the high technology companies are collaborating as a

strategic alliance known as the AGMA (The Alliance for Gray Market and Counterfeit Abatement), a nonprofit initiative to address the gray market threat in the technology industry. Started in 2001 by 3Com, Cisco Systems, Hewlett-Packard, Nortel and Xerox—AGMA is devoted to educate the companies around the globe about the threats posed by gray markets and the effective strategies to combat them. They aim to inform companies about strategies and techniques that will allow the high technology companies to have better monitoring capabilities and approaches that can be implemented promptly to prevent gray market incidents. The role of Information Systems is critical in this process. Therefore, the time is ripe for IS researchers to contribute their insights to address this serious issue. As Information Systems discipline strives to achieve relevance for its research, we believe that the research to prevent IT gray markets represents a truly “relevant topic.” We wish that our work presents a modest start and motivates several others to join the bandwagon.

ACKNOWLEDGMENTS

We would like to thank Sreedhar Madhavaram for his valuable feedback and insights on a previous draft of this article.

REFERENCES

Editor's Note: The following reference list contains hyperlinks to World Wide Web pages. Readers who have the ability to access the Web directly from their word processor or are reading the article on the Web, can gain direct access to these linked references. Readers are warned, however, that:

1. These links existed as of the date of publication but are not guaranteed to be working thereafter.
2. The contents of Web pages may change over time. Where version information is provided in the References, different versions may not contain the information or the conclusions referenced.
3. The author(s) of the Web pages, not AIS, is (are) responsible for the accuracy of their content.
4. The author(s) of this article, not AIS, is (are) responsible for the accuracy of the URL and version information.

Apple Support Communities (2011) “Gray Market Victim”, <https://discussions.apple.com/message/3178184?messageID=3178184> (current June 19, 2011).

AGMA (2003) “New KPMG Survey Projects Global Gray Market of \$40 Billion for Information Technology Manufacturers”, The Alliance for Gray Market and Counterfeit Abatement, http://www.agmaglobal.org/press_events/KPMG%20Gray%20Market%20Release.pdf (current May 21, 2011).

AGMA (2007) “Strategies to Combat Gray Market Diversion Across Your Supply Chain”, *Best Practices in Brand Protection Webinar Series*, http://www.opsecsecurity.com/files/Xerox_Gray_Market_Webinar.pdf (current Nov. 3, 2010).

AGMA (2008a) “Three Keys to Effectively Addressing the Unauthorized Reseller Market”, The Alliance for Gray Market and Counterfeit Abatement, http://www.agmaglobal.org/press_events/FINAL%20Unauthorized%20Market%20Tips%20EMEA%20DRAFT%203-31-08%20doc.pdf (current Aug. 20, 2010).

AGMA (2008b) “KPMG/AGMA Survey Projects Global Gray Market of \$58 Billion for Information Technology Manufacturers”, The Alliance for Gray Market and Counterfeit Abatement, http://www.agmaglobal.org/press_events/12-11-08%20KPMG%202nd%20release%20for%20WP.pdf (current Aug. 20, 2010).

AGMA (2011) “Intellectual Property Rights Take Center Stage in Several Recent Court Rulings”, The Alliance for Gray Market and Counterfeit Abatement, <http://www.marketwire.com/press-release/intellectual-property-rights-take-center-stage-in-several-recent-court-rulings-1518249.htm> (current June 18, 2011).

Ahmadi, R., and B.R. Yang (2000) “Parallel Imports: Challenges from Unauthorized Distribution Channels”, *Marketing Science* (19)3, pp. 279–294.

Aitoro, J.R. (2007) “Fakes: Can You Tell the Difference?”, *CRN*, <http://www.crn.com/news/channel-programs/201800577/fakes-can-you-tell-the-difference.htm?pgno=1> (current May 21, 2011).

Alston, R. (2001) “ACCC Finds Consumers Ripped Off by Parallel Import Restrictions”, Media release by Senator Richard Alston, http://www.dbcde.gov.au/Article/0,,0_4-2_4008-4_15616,00.html (current May 21, 2011).

Antia, K.D., et al. (2006), “How Does Enforcement Deter Gray Market Incidence?”, *Journal of Marketing* (70) January, pp. 92–106.

Antia, K.D., M.E. Bergen., and S. Dutta (2004) “Competing with Gray Markets”, *Sloan Management Review* (46)1, pp. 63–69.

- Assmus, G., and C. Wiese (1995) "How to Address the Gray Market Threat Using Price Coordination", *Sloan Management Review* (36)3, pp. 31–41.
- Bannister, H. (1985) "Gray Market Gets Legal Boost", *Info World*, June 17, pp. 21–22.
- Beth, S., et al. (2003) "Supply Chain Challenges: Building Relationships", *Harvard Business Review* (81)7, pp. 64–73.
- BizForum (2011) "Fighting High Technology Counterfeiting with High Technology Solutions", *New Momentum, Inc.*, <http://www.bizforum.org/whitepapers/newmomentum.htm> (current May 21, 2011).
- BSA, Business Software Alliance (2003) "Eight Annual BSA Global Software Piracy Study—Trend in Software Piracy 1994–2002", http://www.bsa.org/country/Research%20and%20Statistics/~media/Files/Research%20Papers/GlobalStudy/2003/IPR_GlobalStudy2003.ashx (current May 11, 2011).
- Burke, S. (2005) "HP's Hurd Chides Partners Using Gray Market Parts", *CRN*, <http://www.crn.com/news/components-peripherals/175001085/hps-hurd-chides-partners-using-gray-market-parts.htm> (current May 23, 2011).
- Caron, F. (2011) "Valve Locking Out User Accounts for Incorrect Territory", *Ars Technica*, <http://arstechnica.com/gaming/news/2007/10/valve-locking-out-user-accounts-for-incorrect-territory.ars> (current June 18, 2011).
- Deloitte (2010) "When Channel Incentives Backfire", *Deloitte LLC*, www.deloitte.com/.../us_aers_FOCT_AGMA/When%20channel%20incentives%20backfire.pdf (current May 21, 2011).
- Donnelly, D.E. (1997) "Parallel Trade and International Harmonization of the Exhaustion of Rights Doctrine", *Santa Clara Computer and High Technology Law Journal* (445), pp. 447–448.
- Duhan, D.F., and M.J. Sheffet (1988) "Gray Markets and the Legal Status of Parallel Importation", *Journal of Marketing* (52)3, pp. 75–83.
- Economic Times (2008) "Parallel Imports of IT Products Declines up to 20 PC", *The Economic Times*, <http://economictimes.indiatimes.com/articleshow/3255065.cms> (current May 23, 2011).
- Elmer-DeWitt, P. (2011) "Inside the iPad 2 Gray Market", *CNN Money*, <http://tech.fortune.cnn.com/2011/03/14/inside-the-ipad-2-gray-market/> (current May 21, 2011).
- Fletcher, O. (2010) "Amazon Kindle Hits China's Gray Market", *PC World*, http://www.pcworld.com/article/192836/amazon_kindle_hits_chinas_gray_market.html (current Aug.20, 2010).
- HP (2003) "HP Recovers More Than \$1.8 Million in Gray Market Fraud Case", Hewlett Packard, <http://www.hp.com/hpinfo/newsroom/press/2003/030814a.html> (current May 21, 2011).
- HP (2008) "HP Reaches Settlement in Gray Market Case Against Maxicom PC Inc.", Hewlett Packard, <http://www.hp.com/hpinfo/newsroom/press/2008/080311a.html> (current Aug. 20, 2010).
- Kanellos, M. (2006) "Intel's Middle East Gray Market Tussle: Rumors Worse Than Evidence", *CNET News*, http://news.cnet.com/8301-10784_3-6084696-7.html (current May 21, 2011).
- Kessler, M. (2006) "Some See Red Over Gray-Market Goods", *USA Today*, http://www.usatoday.com/tech/products/2006-12-10-gray-market_x.htm (current June 18, 2011).
- KPMG (2008) "Effective Channel Management Is Critical in Combating the Gray Market and Increasing Technology Companies' Bottom Line", *KPMG LLP*, www.kpmg.com/Global/.../Effective-channel-management-gray-market.pdf (current May 21, 2011).
- Lansing, P., and J. Gabriella (1993) "Clarifying Gray Market Gray Areas", *American Business Law Journal* (31), pp. 313–337.
- Li, C., and K.E. Maskus (2006) "The Impact of Parallel Imports on Investments in Cost-Reducing Research and Development", *Journal of International Economics* (68), pp. 443–455.
- Li, Y. (2002) "Pushing for Greater Protection: The Trend Toward Greater Protection of Intellectual Property in the Chinese Software Industry and the Implications for Rule of Law in China", *University of Pennsylvania Journal of International Economic Law* (23)4, pp. 637–661.
- Mark Monitor (2011) "Epson Deploys Integrated MarkMonitor Solution for Global Brand Protection", *MarkMonitor*, www.markmonitor.com/download/cs/cs_epson.pdf (current May 23, 2011).
- Maskus, K.E. (2000) "Parallel Imports", *The World Economy: Global Trade Policy* (23), pp. 1269–1284.

- McDougall, P. (2007) "Microsoft Sues to Block Gray Market Software Trade", *Information Week*, <http://www.informationweek.com/news/198702207> (current May 21, 2011).
- Michael, J. (1998) "A Supplemental Distribution Channel? The Case of U.S. Parallel Export Channels", *Multinational Business Review* (6)1, pp. 24–35.
- Microsoft (2011) "How to Tell—Learn, Verify & Buy with Confidence", <http://www.microsoft.com/en-us/howtotell/default.aspx> (current May 23, 2011).
- Moltzen, E.F. (2003) "No Gray Area: RLM Quits as Intel Distributor", *CRN*, <http://www.crn.com/news/channel-programs/18830228/no-gray-area-rlm-quits-as-intel-distributor.htm> (current May 21, 2011).
- Myers, M.B. (1999) "Incidents of Gray Market Activity Among U.S. Exporters: Occurrences, Characteristics, and Consequences", *Journal of International Business Studies* (30)1, pp. 105–126.
- Myers, M.B., and D. Griffith (1999) "Strategies for Combating Gray Market Activity", *Business Horizons*, November–December, pp. 2–8.
- Nambiar, K.R. (2007) "Intel Takes Steps to Slow Gray Market", *CRN*, <http://www.crn.com/news/components-peripherals/201800981/intel-takes-steps-to-slow-gray-market.htm> (current May 21, 2011).
- Nortel (2011a) "Reseller Agreement", Nortel Communications, http://www.nortel.com/prd/ecpp/collateral/cala_reseller_agreement.pdf (current, Mar. 22, 2011).
- Nortel (2011b) "Reseller Agreement", Nortel Communications, <http://www.norteccommunications.com/pdfs/GreyMarket.pdf> (current, Mar. 22, 2011).
- Nortel (2011c) "Partner Locator", http://www38.nortelnetworks.com/nn/locator/locator_country.asp (current, May 23, 2011).
- Portnova, M. (1998) "Comment: Ownership and Enforcement of Patent Rights in Russia: Protecting an Invention in the Existing Environment", *Indiana International & Comparative Law Review* (50)5, pp. 508–509.
- Rosenbloom, B., and R. Anderson (1985) "Channel Management and Sales Management: Some Key Interfaces", *Journal of the Academy of Marketing Science* (13)3, pp. 97–106.
- Rowley, F.A. (1998) "Dynamic Copyright Law: Its Problems and a Possible Solution", *Harvard Journal of Law and Technology* (11), pp. 481–528.
- Sayer, P. (2010) "Court Must Reconsider EU Parallel-Import Server Sales Ruling", *IT News*, <http://www.itnews.com/drives/21733/court-must-reconsider-eu-parallel-import-server-sales-ruling> (current May 21, 2011).
- Shen, X. (2005) "A Dilemma for Developing Countries in Intellectual Property Strategy? Lessons from a Case Study of Software Piracy and Microsoft in China", *Science and Public Policy* (32)3, pp. 187–198.
- Singer, M. (2003) "HP Nets \$1.8M in Gray Market Case", *Internet News*, <http://www.internetnews.com/bus-news/article.php/3064261/HP-Nets-18M-in-Gray-Market-Case.htm&rls=com.microsoft:en-us&ie=UTF-8&oe=UTF-8&startIndex=&startPage=1> (current May 21, 2011).
- Singer, M. (2005) "Gray Market a Double-Edged Sword", *Internet News*, <http://www.internetnews.com/bus-news/article.php/3462561/Gray-Market-a-Double-Edged-Sword.htm> (current May 23, 2011).
- Steam (2011) "Game Not Available in Your Territory", *Steam*, https://support.steampowered.com/kb_article.php?p_faqid=461 (current June 18, 2011).
- Sugden, D.R. (2009) *Gray Markets*, New York, NY: Oxford University Press.
- Swanson, T.R. (2000) "Combating Gray Market Goods in a Global Market: Comparative Analysis of Intellectual Property Laws and Recommended Strategies", *Houston Journal of International Law* (22)2, pp. 328–368.
- Tomlinson, D.E (1999) "Intellectual Property in the Digital Age: The Piracy/Counterfeiting Problem and Antipiracy and Anticounterfeiting Measures", *Currents: International Trade Law Journal* (3), p. 6.
- Valve (2011) "Steam Surpasses 30 Million Account Mark", *Steam*, <http://store.steampowered.com/news/4502/> (current June 18, 2011).
- Wright, P. (2007) "Protecting Against Gray Market and Counterfeit Goods", CISCO, http://blogs.cisco.com/news/comments/protecting_against_gray_market_and_counterfeit_goods/ (current Aug. 20, 2010).
- Zarley, C. (2006) "HP, Partners Exchange Jabs Over Gray Market", *CRN*, http://www.crn.com/news/components-peripherals/189501153/hp-partners-exchange-jabs-over-gray-market.htm;jsessionid=4BuruxsrktnSxyxWXtOGYQ**.ecappj02 (current May 23, 2011).

ABOUT THE AUTHORS

Dr. Naveen Gudigantala is an Assistant Professor in Operations and Technology Management area at the University of Portland. Naveen received his Ph.D. in Management Information Systems from Texas Tech University. His research interests include Web-based decision support systems, online consumer decision-making, and gray markets for IT products. His research has appeared or forthcoming in journals such as *Decision Support Systems*, *International Journal of Information Management*, and *International Journal of E-Business Research*, among others.

Dr. Pelin Bicen is an Assistant Professor of Marketing at the Penn State University Erie, Black School of Business. In her research, she investigates international marketing strategies, and intra- and inter-organizational new product development activities of firms. Her research has been published in *International Journal of Retail and Distribution Management*, *Journal of Marketing Education*, and *Journal of Business and Industrial Marketing*. She has also presented her research in many national and international conferences and workshops.

Copyright © 2011 by the Association for Information Systems. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and full citation on the first page. Copyright for components of this work owned by others than the Association for Information Systems must be honored. Abstracting with credit is permitted. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or fee. Request permission to publish from: AIS Administrative Office, P.O. Box 2712 Atlanta, GA, 30301-2712, Attn: Reprints; or via e-mail from ais@aisnet.org.



Communications of the Association for Information Systems

ISSN: 1529-3181

EDITOR-IN-CHIEF
Ilze Zigurs
University of Nebraska at Omaha

CAIS PUBLICATIONS COMMITTEE

Kalle Lyytinen Vice President Publications Case Western Reserve University	Ilze Zigurs Editor, CAIS University of Nebraska at Omaha	Shirley Gregor Editor, JAIS The Australian National University
Robert Zmud AIS Region 1 Representative University of Oklahoma	Phillip Ein-Dor AIS Region 2 Representative Tel-Aviv University	Bernard Tan AIS Region 3 Representative National University of Singapore

CAIS ADVISORY BOARD

Gordon Davis University of Minnesota	Ken Kraemer University of California at Irvine	M. Lynne Markus Bentley University	Richard Mason Southern Methodist University
Jay Nunamaker University of Arizona	Henk Sol University of Groningen	Ralph Sprague University of Hawaii	Hugh J. Watson University of Georgia

CAIS SENIOR EDITORS

Steve Alter University of San Francisco	Jane Fedorowicz Bentley University	Jerry Luftman Stevens Institute of Technology
--	---------------------------------------	--

CAIS EDITORIAL BOARD

Monica Adya Marquette University	Michel Avital University of Amsterdam	Dinesh Batra Florida International University	Indranil Bose University of Hong Kong
Thomas Case Georgia Southern University	Evan Duggan University of the West Indies	Mary Granger George Washington University	Åke Gronlund University of Umea
Douglas Havelka Miami University	K.D. Joshi Washington State University	Michel Kalika University of Paris Dauphine	Karlheinz Kautz Copenhagen Business School
Julie Kendall Rutgers University	Nancy Lankton Marshall University	Claudia Loebbecke University of Cologne	Paul Benjamin Lowry City University of Hong Kong
Sal March Vanderbilt University	Don McCubbrey University of Denver	Fred Niederman St. Louis University	Shan Ling Pan National University of Singapore
Katia Passerini New Jersey Institute of Technology	Jan Recker Queensland University of Technology	Jackie Rees Purdue University	Raj Sharman State University of New York at Buffalo
Mikko Siponen University of Oulu	Thompson Teo National University of Singapore	Chelley Vician University of St. Thomas	Padmal Vitharana Syracuse University
Rolf Wigand University of Arkansas, Little Rock	Fons Wijnhoven University of Twente	Vance Wilson Worcester Polytechnic Institute	Yajiong Xue East Carolina University

DEPARTMENTS

Information Systems and Healthcare Editor: Vance Wilson	Information Technology and Systems Editors: Sal March and Dinesh Batra	Papers in French Editor: Michel Kalika
--	---	---

ADMINISTRATIVE PERSONNEL

James P. Tinsley AIS Executive Director	Vipin Arora CAIS Managing Editor University of Nebraska at Omaha	Sheri Hronek CAIS Publications Editor Hronek Associates, Inc.	Copyediting by S4Carlisle Publishing Services
--	--	---	--

