http://www.itbusinessedge.com/images/itbe_logo.jpg

**China Remains Top Source of Counterfeit Tech Goods, Industry Group Says**

1/11/16

By: Don Tennant

<http://www.itbusinessedge.com/blogs/from-under-the-rug/china-remains-top-source-of-counterfeit-tech-goods-industry-group-says.html>

As a technology journalist working in Hong Kong throughout the 1990s, I witnessed firsthand the rampant piracy of U.S. software products, an unabashedly open and institutionalized peddling of stolen intellectual property. While that activity might not be quite as brazen now as it was then, [**AGMA**](http://www.agmaglobal.org/cms/), a non-profit organization of tech companies focused on IP protection in the high-tech industry, says China remains the largest source of counterfeit technology products in the world.

Some years after my return to the United States, [**I wrote a column about my experience in Hong Kong covering the software piracy issue there**](http://www.computerworld.com/article/2558949/enterprise-applications/opium-wars.html). Here’s an excerpt from that column:

On a July afternoon in 1995, I did something that, in hindsight, was pretty stupid. I decided to do a photographic expose on the Golden Arcade, the notorious basement-level maze of shops and stalls in the Sham Shui Po district of Hong Kong that was widely known as the heart of the region's counterfeit software industry. For around $5 to $10, you could buy just about any piece of software imaginable, from operating systems to relational databases to video games. And more often than not, the pirated version of any given U.S. software product was available in the arcade before the legitimate version was officially launched in Hong Kong.

Taking photographs in the Golden Arcade was risky. There were signs posted everywhere showing a camera with a big X over it, with written warnings that photography was strictly prohibited. It was no secret that Hong Kong's triads—organized criminal elements—were heavily involved in the piracy trade, so the signs carried some serious clout.

It was hardly surprising, then, that I raised a ruckus when, once inside, I began snapping photographs. People were shouting, and a Westerner who was paying for his illegal wares scowled at me. ‘That'll get you into real trouble,’ he said. ‘Very trouble,’ a shopkeeper echoed in broken, but effective, English. I ignored them, took a few more photographs, and left without incident.

It is with that experience under my belt that I recently became acquainted with the activities of AGMA, [**whose charter addresses four intellectual property threats:**](http://www.marketwired.com/press-release/agma-weighs-in-on-the-global-battle-against-counterfeits-in-the-tech-sector-2067489.htm) gray marketing; counterfeiting; service and warranty abuse; and digital IP fraud, which is the use of false credentials or identity to obtain IP. I had the opportunity to interview AGMA via email, with responses provided by AGMA board members from Microsoft, APC and HP. For starters, I noted that when I was in Hong Kong I covered the antipiracy activities of the [**Business Software Alliance**](http://www.bsa.org/), and I asked whether combating software piracy is still the purview of the BSA, and if this is also part of the mandate of AGMA. The response:

BSA is still a strong player in business software protection. There are overlapping interests amongst the groups that focus on IP protection in the industry. AGMA looks at issues across IP protection fronts, which include some focus on business software protection, but also on consumer software, computers, and other devices. We have a major focus on supply chains and channels, and the impact in particular of gray market on the industry and society.

I had no idea that service and warranty abuse is an issue, or even what it is. AGMA explained it this way:

Warranty and service abuse refers to use of services, reimbursement for services, replacement of parts, or replacement of products to which the client or end user is not entitled. Every original equipment manufacturer or service provider faces the risk of such warranty and service abuse, and should be prepared to protect its brand by proactively identifying, investigating, and mitigating fraudulent services and warranty delivery. They should plan to take affirmative actions to recover associated losses and facilitate the prevention of future losses. The submission of fictitious warranty claims is the most common fraud scheme, and companies relying on aging systems are particularly exposed to it.

AGMA went on to explain how the organization is fighting the problem:

AGMA members have extensive knowledge of warranty and service abuse, and are sharing this knowledge throughout the high-tech industry through conferences, white papers, and more. The best practices shared within AGMA forums raise awareness and educate the industry on serious issues, which has a positive impact on combating the threats.

As for gray-market and counterfeit products, AGMA’s advice for end users to help ensure that they’re not purchasing those products is to avoid buying products from sellers on the Internet, and to always purchase from an authorized distributor. According to AGMA, users should check the manufacturer's website for the names of authorized distributors, since some sellers make false claims in that regard.