

Fighting Global Brand Counterfeiting and Piracy Using Proactive Intelligence

“Using Logistics Data and Analytical Techniques to Detect Patterns and Anomalies to Interdict Goods in Transit”

Presented at the Annual Meeting

of the

International Trade Mark Association

May 6-10, 2006

Toronto, Canada

By

Dale C. Hogue, Sr

Michael Bednarek, Esq.

I. Introduction

Law enforcement, political leaders and industry are making a concerted effort to counter the production and sale of counterfeit brands, pirated goods and unauthorized brands (third shift). Yet the problem persists and is growing. As all parties struggle to stop these illegal activities, there is considerable harm being done to the world economy and national security is being put at risk by the criminal and terrorist organizations that feed off of the profits from these activities. There is no one simple solution, but a combination of efforts to both interdict the goods and to stop the public from illegally purchasing them would go a long way toward solving the problem. Interdiction efforts must get better in order to stop the flow of illegal goods. It is our goal to assist companies in their interdiction efforts before illegal goods enter commerce or at least before widespread distribution into channels of sale.

II. Logistic Data is the Best Source to Detect and Interdict Counterfeit and Unauthorized Production of Brands

Chasing counterfeit brands at the point of sale or one level up at the distributor level is like chasing rabbits. It keeps investigators and lawyers busy. But is it effective in stopping counterfeit goods from getting to the street?

It is an investigator's goal to extract information from the party caught with illegal goods to gather information on the people and organizations further up the supply chain in order to pursue the case as far as possible. In the best case this results in catching most of the players, but does not completely stop the distribution of the illegal goods. It is more effective to interdict the counterfeits before they are in the wholesale and retail distribution chain.

The practice of using human intelligence from a party caught selling counterfeits and obtaining their cooperation is diminished when the goods are sold over the Internet and the parties selling the illegal goods are not apprehended. In this instance, it is even more important to interdict goods before they reach distribution channels.

The logistics network is the best place to move against counterfeiters. It is a more concentrated collection of goods in transport, usually in bulk, and may provide information that leads directly to the source of counterfeit goods and the networks supporting the supply and distribution of the fakes and third-shift products (unauthorized production of branded goods). The logistics network may be local, national or, more likely, international. Since it inherently relies on documents and data to move goods it is a rich source of data that may be collected and analyzed. Intelligence gathering and analysis techniques are well developed for national security purposes. Using these skills and techniques against counterfeiters and unauthorized sellers of brands can produce information that may be used both civilly and criminally to interdict offending products.

III. Logistics Data Mining and Analysis

Data Collection

Good data is essential to good analysis. Lots of good data is better.

Intelligence is data driven. The quoted axiom is well known in intelligence circles and while it is a simple truth, it is the guiding star of data-based analysis. Fortunately, the logistics world is data rich and mostly accurate unless inaccuracies are introduced which are in themselves telltale signatures meriting attention. A sample of generally available logistics documents for a single shipment are: purchase order, bills of lading, proof of delivery, packing list, custom declaration, equipment releases, load/discharge, cargo status, RFID, GPS/GLS, bookings/conf., manifest, invoices, and bank transactions. There is a huge amount of data in supply chain management systems for any single shipment even in high volume supply chains. All of this data has a snowflake-like effect.¹ At a distance snow flakes look alike. They have much in common such as size and moisture content. Close up they are distinct especially when viewed from different angles. Logistics databases are like a collection of snow flakes. They have much in common but shipments are unique.

The diversity of product shipment makes a single database very large and possibly difficult to manage and mine. It is more meaningful to organize logistics databases by product lines as they have more characteristics in common such as weight, origin, manufacturer, etc. One way to group the databases would be around product categories such as batteries, apparel, accessories, electronics, games, music/videos/games, etc. This suggests that companies in a product line ban together to share and create logistics databases on which analysis may be performed to detect illegal products.

Various U.S. government agencies are involved in using logistics databases for national security purposes. Some of this data may be publicly available. For example, U.S. Customs has a security initiative (C-PAT) using manifest filing timelines and detailed product classifications/descriptions. U.S. Customs is also developing algorithms to spot anomalies in container data and alert for suspect threats. The FDA has a prior notice and facility registration requirement. The DOT has a proof of concept program (Operation Safe Commerce) to monitor the movement of containers. The EU has a pilot program (Contrafic) to monitor high-risk shipments. It may be possible to access some U.S. government databases working in conjunction with the U.S. National IPR Center in Washington, D.C. and like organizations in other countries to build and maintain the databases. The ultimate goal is real time data on which to perform analysis.

Detecting Illegal Goods

We don't know what we know until we know it.

Intelligence analysts examine data to find patterns and anomalies (signatures). The above quote expresses the experience of intelligence analysts that more often than not patterns and signatures are revealed that were not imagined before the analysis began. What is always true of this kind of analysis is that using known data grouping, statistical techniques and analytical algorithms, a robust database reveals its secrets and over time is a powerful predictive tool. The database grows and the through repetitive interrogations it learns and can points its human users to important data, in this case predicting the source and logistics network for illegal goods.

Signature analysis is widely used in civilian and military intelligence organizations in a like manner. U.S. Government Agencies are using analytical techniques to mine their database for defense purposes. The Department of Homeland Security has a program to sift through shipping manifest in its databases and in the future in box sensors to spot threats by looking for anomalies. Database analysis has been used in Iraq to capture terrorist by sorting through known associates and patterns of operations. Law enforcement have created databases and used analytical skills to match criminals to crimes based on patterns.

Likewise, businesses are major data collectors of customer data and sift through it to detect consumer behavior, demographics, buying patterns, score credit worthiness, etc. This type of database mining and analysis exists in every major consumer product company. Supply chain and EDI systems also exist in these corporations, providing a rich starting point for logistics analysis to create patterns of legitimate signatures to measure against. The skill set to interrogate commercial databases is readily available. When this skill is combined with intelligence analysis of logistics data a robust source of information will be produced to detect and interdict illegal goods.

Hogue Management, LLC has created an algorithm to mine and analyze logistics databases. It develops patterns for legitimate shipping activity including data normally used in shipping documents and creates signatures for allowed activity and suspect activity. It correlates this data to known illegal activity to further verify its accuracy. It examines data to detect sources of unauthorized goods in transit and the source of the goods. Data of current activity may be examined by the algorithm to detect unauthorized goods in transit. HM will make this service available to brand owners. HM has applied for a patent on the algorithm.

IV. Next Steps

The authors suggest that interested companies form together, either directly or through an association, to create a combined logistics database and use intelligence analysis techniques to mine the data for use by the members to interdict illegal goods. Michael Bednarek will assist in forming like-minded company product groups to support a database assembly and analysis project. Hogue Management, LLC will provide the database and analytical support using its own resources and that of trusted vendors that it now uses for database management and analytics.

Hogue Management, LLC will also work directly with brand companies to analyze logistics data to spot counterfeit activity and brand diversion.

Biographies and Corporate Data Attached

Contact Information

¹ Presented at the Symposium on Risk in Supply Chains, February 2005, by Dhiren Patel, President, FreightDesk Technologies, Inc.