



The Network Delivers

IT Audit Issues

The Ten Commandments of fighting software pirates?

You mean, as in, “GOD SAYS...”?

This paper was written to discuss and review the information provided in the following article:

The Ten Commandments of fighting software pirates

by Eric Sinrod, CNET News.com Published 6/21/06

<http://techrepublic.com.com/2010-1009-6086062.html>

While I believe that Mr. Sinrod's perspectives are perfectly valid, I would like to consider those same perspectives through the eyes of the business technology consumer and professional software asset managers.

Don't get me wrong. I think the enforcement industry players are performing a function that is as necessary as their process is (to me, at least) ethically questionable. But, these folks are actually giving us Ten Commandments? As in **“THESE ARE THE WORDS OF GOD”**? Hardly... Please accept my apologies as I filter through this article and point out just a few disconnects with the realities reported by hundreds of front line software asset managers from across the globe. Due to space limitations in the feedback section on the TechRepublic web site, I only addressed the first three paragraphs of the article. My reactions to the rest of these so-called commandments are included here.

“...there's light at the end of the tunnel—if only consumers would pay closer attention.”

Precisely who is in this tunnel and what tunnel is it? And, consumers need to pay closer attention to what? It appears that the tunnel we're discussing involves leveraging more and more money out of the collective software consumer's pockets. The view in the consumer tunnel involves getting the most for our money. The copyright holders' tunnel appears to be more focused on controlling the actions and spending of the consumer to ensure long term revenue streams. And what does the light represent? Wouldn't it be great if the light actually represented the light of a mutually beneficial relationship?

Here is a really interesting concept for software industry players: Lower your prices

to match the value that the majority of genuine consumers place on your products. Quit pricing products based on what you believe they're worth—or what your most prosperous (most addicted?) consumers think the products are worth. Want to reduce piracy? Listen to and follow the wishes of the majority of your customers.

“Unwitting consumers at times get duped into buying pirated software online. This results in substantial lost revenue to the true developers of the software while consumers get stuck with sub par applications.”

Those same “unwitting consumers” also buy products from so-called authorized resellers who copyright holders later have to confront for illegally selling products. So, who should the consumers trust? The industry's own (occasionally) dishonest suppliers or those lower-priced suppliers on the net? And would people **PLEASE** quit telling the consumer that they are taking money away from those poor software developers by purchasing product from alternative channels. Does anyone out there honestly believe that, once the code is written & copyrighted, the creative minds behind it get a percentage of sales?

Here is how it seems to be working in the real world. One major software publisher has taken a significant portion (\$18 billion worth) of the intellectual property rights of those poor American developers and transferred it all to Ireland to cash in on lower taxation. This same publisher reports that it is losing approximately \$500 million in piracy per year. And guess what? By moving all of that creative IP out of the U.S. this publisher has cut its taxes on IP assets by over \$500 million. Does anyone want to hazard a guess as to the chances of the additional profits going directly back into the pockets of the hardworking front line developers back in the States who made this company profitable? Or is it more likely that the money is going somewhere else?

“Indeed, one study estimated that 21 percent of software in the United States was unlicensed, accounting for lost revenue of \$6.9 billion.”

Does anyone who understands the concept of “unbiased research” still believe the results of this often quoted study series? Dozens of highly educated and qualified people have peered beneath the shadowed skirts of this specific series of studies and come to the conclusion that they are not accurate, nor are their piles of numbers being interpreted with any degree of accuracy. Quit quoting them as demonstrable facts.

Besides, if you want to put the hammer to piracy, you might want to start concentrating your efforts in China and the former Soviet Union territories where the real incidence of piracy is the most significant. Cutting the disease off at the source isn't a new concept—you may wish to invest a little more effort in doing so. However, we do recognize that confronting a “small” business in China that is

churning out millions of dollars in counterfeit goods is significantly less profitable than suing a small business in the United States that unwittingly purchased three copies.

The rest of this paper addresses each of the ten points in the article. I didn't include it in my TechRepublic commentary due to space limitations.

Commandment: Trust your instincts...

Ah, yes. The old, "if the price is too good to be true, it probably is," routine. Frankly, this concept no longer works: Not when the office suite of one major enforcement industry player is selling for nearly \$500USD and the consumer could purchase a comparable product for less than \$100USD. Based upon this commandment's flawed logic, I would suggest that **THAT** \$100 price is certainly too good to be true. Besides, since most intelligent counterfeiters are aware of this old phrase, they also know perfectly well that, "...if the price is too high to be reasonable, the product is most likely genuine..." and they quietly price their counterfeit goods accordingly. (Just doesn't make a great deal of sense, does it?)

Commandment: Make sure it's authentic...

"Be wary of software products that do not include proof of authenticity like original manuals and warranties." Let's take these concepts and dissect them just a little and then view them from the perspectives of the business technology consumer.

First of all, does anyone know precisely which operating systems & software products on the market actually **come** with certificates, stamps, or seals of authenticity and which do not? The vast majority of titles do not include these little items, and for good reason. You see, with today's advanced printing & copying technologies, even a partially talented counterfeiter can create authenticity documents that would easily fool more than 90% of business technology consumers.

Next our self-styled enforcement prophets want consumers to manage original manuals. How many of the operating systems and software products on the market no longer come with publisher-printed manuals? Most of them? In fact, those very same manuals consumers are supposed to check out are usually contained in a text file on the master media. If the counterfeiter has even half a clue of his trade, his illegal copy contains the same digital manual as the genuine original. Well, THAT should be easy for the average consumer to identify, right?

Next, we have the warranty. Anybody out there ever READ the warranty on a new operating system or software product? I'll save you the trouble: The majority of warranties cover pretty much nothing. For the most part, software industry warranties are carefully crafted legal documents relieving the copyright holder of virtually all responsibility and transferring that responsibility onto the shoulders of the consumer. You "might" get your original purchase price refunded, but don't hold your

breath. In addition, the warranty also most frequently arrives at the consumer level within a text file on—you guessed it—the original media. Once again, Jimmy the Counterfeiter simply duplicates the authentic warranty contained on his personal master copy. So? What does the empty warranty have to do with counterfeiting?

And finally, two really interesting “little” details that our courageous group of list-makers seems to have missed: Primarily, the consumer does not get the opportunity to check any of these items until **AFTER** concluding the purchase. The money is already long gone and the company is now stuck with what may, or may not, be valid product. Realistically, as an IT employee or manager, what would you do? Quietly slip the product into operation and hope the question never comes up? Or would you inform executive management that you just threw away a couple grand of corporate funds on questionable products and you would like a few grand more to replace it? Let's see... Job security or professional suicide?

Secondly, the guiding list of “dos & don't s” in this article seems to have neglected to mention that easily forgotten item called a product license. Then again, if the authority documentation is easy for counterfeiters to duplicate, the license should be a cinch, right? Once again, however, consumers do not get to review this item of documentation until **AFTER** the purchase is concluded. Does anyone see a pattern developing, here?

Commandment: Read the label...

I'm sorry but, even the least qualified asset management or purchasing employee already knows that product with a hand written label is not going to be valid. Quit pointing out the obvious. What is the consumer to do if the label is so faithfully printed that it virtually matches the original? Once again, the vast majority of consumers wouldn't have a clue, unless the counterfeiter was completely incompetent. And, once again, the consumer has already spent the money, is stuck with the product, and is now in a very hazardous professional position. But, I'm sure the boss will understand. Just walk into the office & tell her what happened. (Go right ahead.) Are the patterns emerging for you yet?

Commandment: Beware of backups...

Highly effective and professional resellers quite frequently offer to back up your systems before delivery. This way, if a system fails or you trash one, the replacement can immediately be brought into line with your previous configuration. Although this point may be valid, it is probably the least credible of the entire list—unless, that is, if your supplier sends you the backup copies instead of the original media. THEN, you can start asking the tough questions, like: “Will the boss understand this?” More patterns emerging?

A second, and very valid, risk with backups is that even highly qualified technicians sometimes back up an entire hard drive—rather than only the documents. Whenever

a system is completely duplicated on a backup server there is an enormous danger that full applications have been backed up, too. When your personnel back up the entire application the chances are extremely good that you have violated copyright.

Hint: If any application can be executed (started) from the backup media that application will require another license.

Real World – My team worked an audit for a company targeted by an enforcement group. We discovered that an employee had backed up his entire hard drive to the server—not once—but six times. Essentially—technically—every copyrighted product on that computer was illegally loaded on the server six times. Big mistake...

Commandment: Steer clear of compilations...

Absolutely. If you purchase any copyrighted product and it turns out to be a collection of products piled onto a single master CD, you have just been handed a very unsavory bag to hold. In this case, there isn't much to do but document your actions and destroy the product. Need I even mention that you should **not** make use of this CD?? Again though, once the money is gone, it is gone.

Commandment: Look for the trust mark...

Let's see: the license can be duplicated, the authenticity documents can be faked, the warranty and master media can be counterfeited, and industry approved resellers can deliver fake product, right? Well, **HERE'S** a useful answer: Create yet another mark, seal, stamp, document, or certificate for the counterfeiter to duplicate with technological ease. After all, once the purchase is made and the consumer is locked into the product, that trust mark will certainly help them identify where they went wrong, right? This concept ranks right up there with passing yet another copyright law to further duplicate all the other laws already on the books. What's more, we're all aware of how happily the reseller will refund your money. Patterns & processes...

Commandment: Do your homework...

Review the feedback sections of the seller sites. After all when that Fortune 100 buyer gets bilked for \$50K worth of hot product, he will jump right out on the site and report what happened. And, of course in doing so, he'll tell the entire world—including the enforcement industry players—that he is now in possession of illegal product. I think we can call this one a tie for first place in pretty illogical list creation reasoning, don't you? In the history of technology, people and companies simply do not admit they have been hacked, cheated, or bamboozled in any manner. Don't cross your fingers in the hopes of avoiding a product due to customer feedback.

Commandment: Get the seller's address...

Okay. Forget what I just said. The other two commandments are tied for second

place. **THIS** little gem just blasted into first place as the least logical and least intelligent list item. Get their address? There is absolutely no doubt in my mind that a person who is skilled enough to counterfeit all of the documentation and media for the illegal product you just purchased will be willing to give you their home address. What are your thoughts on the matter? Or is this just one more case of emerging pattern recognition?

Commandment: Keep receipts...

You bet your overpriced, feature bloated, patch managed, copyrighted product assets that I'm going to keep my receipts and purchase documents. Of course, when the CIA traces the documents back to a bombed out field in Lower Pavlovia, I'm certain that all the documentation will help me get that refund I have coming. Or, at the very least, they empower the enforcement industry player's legal accusations that I am guilty of receiving stolen or counterfeit goods. Patterns? You bet.

Side note...

"...retain copies of your order and sales confirmations at least until you have confirmed that purchased software is legal and not pirated." Who in the world wrote this list? Any technology asset management professional who is even partially trained is well aware that the purchase documentation for copyrighted products is always retained for the life of the product and all related products. For this list to even vaguely imply that one only needs to keep documentation until the product is confirmed legal is enough to qualify this statement as candidate for a first place tie in our sloppy list profile. Pattern? You bet your software assets there's a pattern here. Without that clear and detailed purchase trail, your company will fall prey to any enforcement audit now or in the future. If you cannot conclusively prove that you paid for the product, it doesn't matter much if the product is counterfeit or not, you cannot prove you obtained it legally.

Commandment: Be careful when crossing the border...

This one is actually pretty useful. It is a confirmed fact that a great deal of counterfeit products are being produced in the so-called developing countries. Those products are, indeed, being heavily marketed on the Internet. We'll let this list item slide because it is probably the most credible item on the list. BUT, there is still a pattern, here and it is not in favor of the business technology consumer.

Alright? Those are the "Ten Commandments" of fighting software piracy. I know that I hammered these concepts pretty hard, and I apologize if I've wounded anyone's pride or delicate sensitivities. However, as the enforcement industry players continue to imply, the only way to get the message through is to ensure it has impact. So? This is my perspective. Here are some of my suggestions for cutting the impact of piracy in your company.

For the business technology consumer:

1. Establish and enforce strict policies & procedures for technology acquisitions. Any product that is acquired outside those procedures will be immediately removed when discovered. Any personnel introducing any unauthorized technologies into the enterprise will be disciplined with penalties up to and including termination. Document every step of every event.
2. Establish and enforce a strict & comprehensive documentation and copyrighted product portfolio management process. Always be less than twenty-four hours from current statistics detailing what products are loaded, where they are loaded, who uses them, and who is a member of the technical support and utilization cycle.
3. Do not purchase any copyrighted product without negotiating clear license and documentation. Ensure that all purchase documentation is closely reviewed by a qualified software compliance manager or asset manager prior to paying for the product—no matter who sells it to you. Document the process for each acquisition.
4. Only purchase from recognized suppliers and periodically check up on those suppliers with the copyright holder to ensure that you do not become entangled in sharp practices. In most cases, do not purchase from a supplier outside the country where you intend to license the product. Document the steps you take to ensure supplier credibility and expect the copyright holder to confirm, in writing, the status of the supplier.
5. Inspect & secure all master media & documentation immediately upon receipt. Only qualified personnel are permitted to check out master media and they must submit installation documentation to confirm their use.
6. Do not purchase any software products online without confirming with the copyright holder that the supplier is a valid reseller. Never...NEVER purchase shrink wrapped product for corporate use and NEVER, ever permit employees to download licensed products from the Internet.
7. Conduct periodic automated audits of your systems and reconcile the results with the products you are legally entitled to possess. Conduct random automated spot audits in between scheduled ones.
8. Very closely monitor and ensure the legal process behind every upgraded product, every transition between evaluation product and full license, and every shareware installation. Closely document any copyrighted product as it moves into through and out of the tech environment.
9. There are more but these will get you started... Those who wish to review additional processes, let's discuss on the Forum or you might want to attend my asset management training.
10. Of course, we could all switch to open source & eliminate the limitations of proprietary products...

For copyright holders and their enforcement friends:

1. Your customers are not your enemy. Work toward establishing mutually beneficial solutions to piracy issues, not punitive events.
2. Target the people and groups who produce the counterfeit, pirated products. Shut them down. Disrupt & destroy their supply chain options. Work to cure the disease, not the symptoms.
3. Quit massaging the truth to fit your perspective. Consumers are not dumb and, like you, they resent being treated as if they don't have the sense to recognize a scam. If it's all about money, then admit it. If it is about ethics, then show that you have them yourselves before expecting others to change theirs. If you don't have the truth, help find it.
4. If you conduct studies and/or research, do not conceal the processes involved in developing the output. If the study is accurate to +/- 20%, say so in order that folks more clearly understand the credibility of the figures.
5. When a customer makes a licensing mistake, work out a customer relationship centered solution. Don't jump to threats of litigation. Has it crossed anyone's mind that maybe the piracy rate is being influenced by attitude?
6. Make acquisitions and licensing easy and convenient for the consumer, not just for yourself. Simplify license Ts & Cs. Give the consumer some rights and take responsibility for your products. If people do not understand the agreements, they will not follow them. If they sense that the agreement ignores their specific needs, they will bypass the terms.
7. Adjust prices to match the actual value of the product to the specific consumer culture. Consider the Big Mac index. Eliminate feature bloat and produce products that do the job instead of justify ever increasing price tags. When you reduce functionality to reflect actual requirements, don't label the product "crippled".
8. If your product is full of holes and defects, fix them before you put the product on the streets. If you continue to insist that your consumer conduct the quality testing that you don't conduct, reduce the price to reward them for their troubles.
9. More? We have plenty more, but changing just these few processes would revolutionize the industry.

We are all very well aware that the vast majority of copyrighted products companies work hard to develop & deliver quality products and services at competitive prices. Unfortunately, a difficult minority in any endeavor can taint the industry for the rest. The technology industries have changed the world. However, that does not mean that we can't work cooperatively to enable even more and better changes down the road.

Here's a Concept:

Let's all begin thinking in terms of mutual benefit...instead of mutual punishment.