

CONFESSIONS OF A CABLE THIEF

BY ANTHONY CRUPI

Cable World, Oct 6, 2003

For someone who looks to be sitting on over \$5,000 in stolen stereo equipment, the short kid in the Michael Vick replica jersey is remarkably relaxed. Maybe it's his proximity to all the other ripped-off merchandise on Canal Street — an exhaust-choked downtown thoroughfare that pretty much functions as Manhattan's large intestine, as far as the stolen goods trade goes — or maybe all the heat is bearing down on the old guys shilling Prada knockoffs up the street, but either way, the kid leaning up against the van is cool.

The same can't be said for his vehicle, a creepy brown van destined to be tossed for DNA evidence before making its last trip to the auto graveyard. But if you're of a certain mind-set, the stuff inside the van more than makes up for its aesthetic shortcomings. Both the rear doors are thrown open, and in the pixelated murk of dusk I can just make out the brand names of some of the components he's got stacked up in the back. Yamaha. Sanyo. Kenwood.

When I ask to take a look at a CD player with a six-disc capacity, Mini Vick makes a face like he's recalling a foul odor. "I can't be opening every box up in here," he grouses, which works as a better sales pitch than you might imagine. Speed is of the essence here. There's really no time to sniff at the merchandise or haggle over the price. As a crowd of consumer electronics enthusiasts begins to form on the periphery of the Crimemobile, I clear my throat and ask for what I really came for.

"You got anything in there that will get me free cable?"

Five minutes later I'm \$20 lighter. I've got a standard-sized padded mailer stuffed into my messenger bag, though I opted to leave the CD player behind. No need to compound the felony.

That said, I'm already pretty sure that I've been ripped off. Without going into too much compromising detail, on the few occasions in the (far distant) past where I have been a party to, uh, signal reallocation, there was always some kind of set-top-type device involved. Something rectangular and substantial, with an LED readout on the front and a port or two in the back. What I have in my possession right now seems a little on the slight side.

My suspicions are confirmed on the 6 train. When I tear open the package, I find two cylindrical metal objects with threaded endpoints and the legend "CT-HPF" stamped on each. HPF is merely an acronym for "high pass filter," a device that reduces signals received from transmitters operating below 30 MHz. Your cost at Radio Shack: \$3.95. Damn you, Mini Vick.

Of course, it's hard to get self-righteous about being thwarted in an attempt to break the law. My getting burned on a cheap piece of hardware is nothing compared to the fleecing the cable industry's been taking since the days of the Jerrold box. A comprehensive survey conducted by the National Cable & Telecommunications Association in 2000 concluded that revenue lost to cable operators as a direct result of signal theft were in excess of \$6.5 billion a year, or about 17% of the industry's estimated gross. Small potatoes it ain't.

Once those figures started making the rounds, cable's biggest challenge, other than stopping signal theft outright, was to convince the general populace that there was, in fact, something fundamentally wrong about stealing the service.

Trouble is, there seem to be an awful lot of people out there who disagree with that assessment. A Massachusetts-based cable filcher interviewed in *Cable World* last year argued that recent news about the accounting practices of his service provider (Adelphia) justified ripping off the signal.

"The way I see it, I'm just thieving from the thieves," he said. "When they clean up their act, maybe I'll clean up mine."

That may be a weird inversion of the Golden Rule, but this kind of moral opportunism isn't limited to Adelphia's service footprint. Google the phrase "free cable," and you'll find yourself staring down the barrel of 263,000 hits. The more specific query for "cable descrambler" yields 81,100 hits. We're a nation of thieves.

Much of the casual attitude toward cable theft can be traced to two co-related factors. Firstly, there are a lot of people out there who really have a strong aversion toward their local cable provider. After years of being jerked around on installation and service calls ("We can get there three Mondays from now, between 8 a.m. and 6 p.m."), customers began to view the cable company with the same enmity once reserved for the federal government. "Once satellite got their foot in the door, people got a lot more grouchy," says Carey Turner, a former Adelphia field technician. "Now that cable's monopoly is busted up, across the board you're seeing a greater effort to serve the customer more quickly and more effectively."

Secondly, it's rather hard to turn up what is in effect a free lunch. In his experience, Turner guesses that most cable theft is passive. In areas where there are high seasonal turnover rates — resorts, university towns — the tap to a previous tenant's home may often never be shut off. Thus, when the new tenants move in, they find that they have inherited cable. "You have to go out to the site and physically turn the tap off," Turner explains. "For whatever reason, that doesn't happen as often as it should."

These sorts of situations tend to be handled with a bit more élan than active theft via hacked equipment or illegally spliced lines. The NCTA's Office of Signal Theft advocates a certain amount of tolerance in dealing with illicit cable activity, offering operators a wealth of materials to aid in the development of amnesty campaigns. (The OST prefers the term "no-fault.") It's a soft-sell approach, on the whole. The no-fault package, permutations of which have popped up in various Comcast, Cox and Time Warner systems throughout the country, encourages those who have been stealing cable service to come forward during a proscribed period of time and hand over any unauthorized descramblers or filters without fear of prosecution. The goal is to convert the thieves into paying customers; judging by the OST's promotional materials, they're not above invoking shame to speed the process along. (The bill stuffers and door hangers in the amnesty toolkit feature seemingly well-adjusted citizens juxtaposed over captions that read, "Funny — he doesn't look like a thief." Sew-on scarlet letters sold separately.)

Which is not to say that the NCTA doesn't promote a little hardball when circumstances merit. Like the last, almost innocuous clause in the government warning on a beer can ("...and may cause health problems"), the association fires its big guns almost as an afterthought: "Using state and federal theft of service laws when appropriate." The penalties can be severe.

Offenders can be charged either with a Class B infraction, which carries a fine of as much as \$1,000, or a Class D felony, punishable by six months to three years in jail and a fine of up to \$10,000.

Anybody who finds himself behind that particular eight ball would do well to throw themselves on the mercy of their local provider. During a recent two-week period, Comcast offered amnesty to residents in parts of its Maryland/Delaware division. According to Comcast spokesperson Kirstie Durr, nearly 5,000 people in the area volunteered to either turn themselves in or elected to point the finger elsewhere.

Because they're looking at a \$6.6 billion sinkhole, cable operators aren't afraid to let others do the heavy lifting for them. An unaffiliated website, <http://911cabletheft.com/>, allows anonymous tipsters to blow the whistle on thieving neighbors and friends via a pull-down menu. The site capitalizes on a grievance that hits closest to home; i.e., the unfairness of it all: "You're paying your bill — Why aren't they?"

Thus far, 15,721 (48%) of those who have responded to the site's quickie poll say that either they or someone they know is stealing cable. There are no indicia to ascertain just how many users have turned themselves or someone else in to the authorities, but if schadenfreude has anything to do with it, we're guessing that the latter beats out the former by a 10-1 margin. (Consider the sentiment behind the "Revenge via Cable Theft Report" message board, which appears to be a forum for people looking to boast about ratting out their close pals.)

So then, back to our experiment. I have in my possession a pair of digital pay-per-view filters. In theory, these things should allow me to be able to grab PPV movies off the network without attracting the interest of the cable company's billing department. Already I'm envisioning a host of difficulties, not the least of which is that I'll need a digital cable set-top box to test the filters out. (No, I don't subscribe to digital cable. Yes, I am full of shame. Let's move on.)

A friend of mine volunteers to sacrifice an evening for the good of this experiment, just so long as I bring beer. This turns out to be a capital idea, as the whole PPV filter thing turns out to be a big nothing. Following the hastily typed instructions that were wedged into the bottom of the mailer, I simply screw one end of the filter into the coax, and the other into the set-top (a Scientific-Atlanta 2200).

It works, but it's all a bit of an anticlimax. This isn't stealing cable, it's ripping off PPV content. (This particular content, a Kevin Spacey-on-death-row snoozer called *The Life of David Gale*, momentarily makes me wish I could trade places with the titular character. Terrible.) Uninspired film choices aside, the central lure of the filter gets radically diminished once I read the disclaimer on the back of the instruction sheet. Roughly translated from what must have been Turkish, the note warns that the "customer MUST let the cable company know that they (sic) are accessing pay-per-view movies!!!" In a similarly exclamatory vein, the note goes on to caution that the "box's memory MUST be cleared before removing the filter!!! The filter stops the box from talking to the cable company, but the receiver will store it. If you remove the filter BEFORE clearing the memory, all your PPV movies will be called in at once!!!"

This elicited some nervous squealing from my friend, who was convinced that the cable cops were going to kick the door in and drag her off to Riker's. Given the option of leaving in the filter and never ordering PPV again or pulling the plug and coughing up the \$3.95, she chose the former.

On my way home, I threw the filters away with the empties.

I took another stab at free digital cable later that week. A quick Google search led me to a New Jersey-based company that claimed to offer a “digital cable descrambler” that looked a lot like the analog descramblers of my youth; \$169 later, and I've discovered the reason for that. Here's where the value of digital can really shine through for the cable operators who have updated 100% of their plant. Besides being able to offer advanced digital services which will eventually begin to eat away the massive infrastructure costs accrued in the upgrade, digital cable offers unprecedented security. N2 Broadband principal architect Darryl DeFreese says that the triple-DES (digital encryption standard) used in digital cable plants offers “military-grade encryption.”

“In a digital environment, information is thoroughly randomized,” DeFreese says. “Each individual frame of video is so well encrypted that to decrypt much of the content that's available to digital subscribers would take more computing power than there is now available in the entire universe.”

In fact, nobody has come close to cracking the triple-DES algorithm. Nor are they likely to. “Sure, if you throw enough pianos into the Grand Canyon, eventually one of them will fall up,” DeFreese muses. “Haven't seen that happen yet, though.”

Even someone advanced enough to hack a digital box that can work across both Motorola and Scientific-Atlanta platforms — and that alone is staggeringly unlikely — wouldn't be able to prevent the inevitable service call when the customer's signal falls silent for a period of time. What's more, the odds of being detected through the sort of signal leakage that is associated with a hacked box can't be completely ignored.

Speaking of which, DBS, the threat that can never be ignored, has taken a much tougher stance on theft than its earthbound rivals. Because its access cards are relatively easy to clone, DirecTV tends to put the squeeze on anyone it suspects of signal piracy as soon as any such information is forthcoming. And while there has been some concern that the new CableCARDS for digital plug-and-play sets will provide an easy target for hackers, the security guys are already three steps ahead of the game.

“Our CableCARDS are highly tamper resistant,” says Tony Wasilewski, chief scientist, Scientific-Atlanta. “There are various physical and logical elements in place to prevent any potential tampering.” Not only are the microprocessors secure from remote attacks — S-A's PowerKey conditional access platform is “unbroken and unduplicated,” Wasilewski says — but an “impermeable membrane” creates a physical layer of security which prevents the cards from being pried open.

Where cable ops see security in digital, some outsiders see a challenge. J., a network specialist who has tackled IP and POTS security issues, immediately identifies the descrambler I bought as an analog box. “That doesn't mean we can't make something of it,” he grins.

Back in the early '90s, J. used his intricate knowledge of encryption to hack his way into targets as ripe as Southwestern Bell's switching facilities in Houston. After getting sent up for 18 months for “illegal computer invasion,” the Brooklyn-born hacker decided to limit his activities to non-felonious pursuits.

But he still likes to take things apart to see how they work. He pops the case of the bum unit and points out various elements of circuitry. From a few inches above, it looks like a road map of Omaha.

"This thing couldn't decrypt a game of Pong," J. says. "You got taken." As his finger traces a path across the guts of the box, the relative simplicity of the thing becomes apparent. All the information needed to form a coherent picture is actually embedded in the analog signal; the box simply hunts around until it finds the signal. It's like having the right key to start your car on a ring with three other keys. There's nothing to it.

Digital? That's like having the right key on a ring with all the keys that ever have and ever will exist.

It's there. Good luck finding it.

© 2003, Primedia Business Magazines and Media, a PRIMEDIA company. All rights reserved. This article is protected by United States copyright and other intellectual property laws and may not be reproduced, rewritten, distributed, disseminated, transmitted, displayed, published or broadcast, directly or indirectly, in any medium without the prior written permission of PRIMEDIA Business Corp.