The theft of video signals has cable-TV and satellite-TV programmers aggressively pursuing signal pirates.

Signal Theft

PAUL PARADISE*

VIDEO SIGNAL THEFT IS NOT NEW. it's hardly sensational, and it's rarely prosecuted. However, the cable-TV industry, by its own estimates, loses billions of dollars each year because of it. As the cable and satellite-TV industries prepare for new interactive technologies, they have become increasingly aggressive in trying to thwart signal pirates.

Perhaps the most dramatic action by a signal pirate was the transmission of the following message that was seen by hundreds of thousands of cable subscribers in the East and Midwest during an HBO cablecast of the movie *The Falcon and the Snowman*: "Good Evening HBO from Captain Midnight. $12.95 a month? No way! (Showtime/The Movie Channel Beware.)"

The sender, who used a satellite uplink to superimpose his message on the HBO transmission, was eventually caught and prosecuted. But his sentiments regarding the rising cost for premium cable television and signal scrambling are shared by many.

In January 1986, HBO and Cinemax, both owned by Time, Inc. became the first two cable programmers to scramble their satellite signals, thereby preventing people who owned satellite-TV reception (or TVRO) systems from watching their programming without paying a monthly subscription fee.

*Excerpted from the forthcoming book: *Designer Counterfeiting*.

In May, 1986 little more than a week after Captain Midnight's pirate broadcast, Showtime and the Movie Channel followed suit and scrambled their signals. Today, virtually all of the major cable networks scramble their satellite feeds.

Despite signal scrambling and a significant enforcement effort by the cable industry and the Motion Picture Association of America (MPAA) to apprehend illegal users, signal theft remains rampant. According to the National Cable Television Association (NCTA), almost one-quarter of all cable viewers in this country do not pay for the service. In 1992, the NCTA estimated that signal theft amounted to a loss to the cable industry of $4.75 billion.

Satellite scrambling history

Signal theft grew in popularity with the growth of the home satellite TV market in the early 1980s. Home TVRO systems first became available in 1979 and were particularly attractive to TV-starved rural residents. At that time, a home satellite system cost $10,000.

In just a few years, the cost for satellite dishes dropped to $2,500, and demand for the dishes surged even in urban areas. Home TVRO systems became a growing concern to programmers. They worried that the availability of consumer satellite-TV systems would cause cable-TV subscriptions to plummet, thus reducing their revenues. The industry sought a way to prevent unauthorized viewers from watching their signals; the result was that programmers scrambled their satellite-delivered signals.

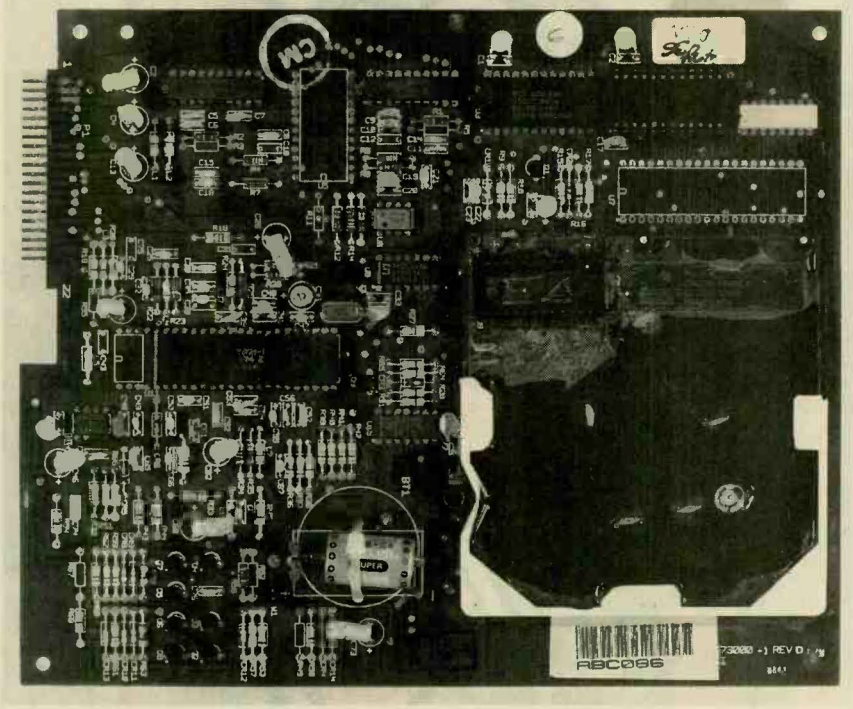
Signal scrambling upset consumers and dealt a major blow to the satellite-TV industry. Sales of satellite systems, which had reached 70,000 a month, fell to fewer than 15,000 a month. The early signal scrambling, however, spawned a new industry: illegal descrambling.

The scrambling method chosen by HBO that became the *de facto* standard for satellite-delivered television was VideoCipher II, developed by M/A-COM. VideoCipher II scrambles the video portion of the signal by replacing the horizontal- and vertical-sync signals with digital data. The digital data stream contains the audio portion of the signal, as well as the authorization codes or addresses of all legitimate descramblers. The digital data are encrypted with the data encryption standard or DES.

Although the DES itself was never "beaten" by signal pirates, VideoCipher scrambling proved to be easy to defeat through several "back doors." Descramblers, for example, were cloned so that a single legitimate subscription could turn on thousands of descramblers.

After pirates had compromised the security of VideoCipher II, General Instrument Corp., which bought the technology from M/A-COM, was forced to develop a new scrambling scheme called VideoCipher II Plus. The Plus system has yet to be successfully "hacked." The most recent version of the scrambling technology is VideoCipher Renewable-Security or VCRS.

The VCRS system has two features that make it resistant to piracy. First, developing a way to defeat the system would require a considerable investment in advanced technology. Second, the VCRS module has a provision to accept smart cards to update the encryption technology to counteract any "hacks" or security breaks. The smart cards can be produced quickly and cheaply, allowing any security breaks to be patched promptly.



THIS EARLY VIDEOCIPHER II BOARD was compromised by signal pirates. Notice that the potting compound has been removed from around the microprocessor and EPROM socket.

Other Satellite piracy

Despite the development of the VCRS that has virtually eliminated signal theft by home satellite-TV viewers, satellite theft remains a serious problem, according to Dennis Powers, Chief of Signal Security, Legal Department of HBO. "The main focus of our signal theft efforts is the commercial misapplication of our satellite signal," said Powers. "We're not necessarily talking about boxes or modules that have been compromised or pirated, but multiple dwelling areas like trailer parks, apartment complexes, and recreational-vehicle parks that have set up their own cable

systems under the guise of being TVRO installations. The pirate is paying a user fee, but is bringing down our signal and then redistributing it throughout the complex and charging a fee to each subscriber."

According to Powers, the illegal user is acting as an illegal distributor or illegal franchisee by selling the programming to other users who may, or may not, realize that he is doing so without authorization.

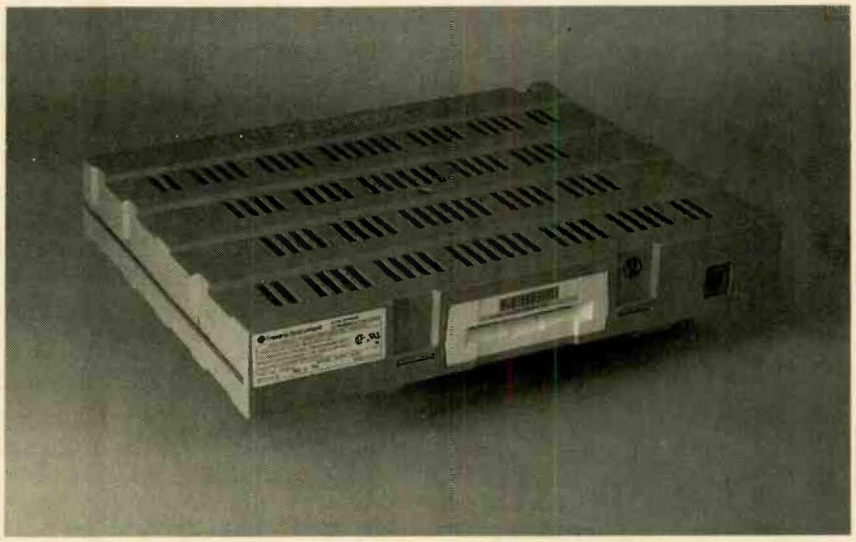
Other forms of satellite theft include sports bars that pick up sporting events not usually available on broadcast channels or cable networks.

Some sporting events that are distributed by satellite are not available in certain "blacked out" areas. For example, Major League Baseball has ruled that out-of-town games should not be made available anyplace where the home team is in action. That means that an avid fan of the San Francisco Giants who lives in New York would not be able to view his favorite team if either the Yankees or Mets were in action. The rules for NFL football prohibit a home game from being televised in the team's region if the stadium isn't sold out 72 hours prior to kickoff.

Such rules can be enforced by VideoCipher, which has the ability to black out programming according to ZIP codes. However, some TVRO system owners have been known to give incorrect address information when ordering program subscriptions so that they could watch programming that would otherwise have been blacked out to them.

Commercial establishments such as sports bars that masquerade as residences have been another problem. In this case, an establishment attempts to reduce its subscription fees by registering for a residential instead of commercial subscription.

Such satellite theft is difficult to trace. Leads for enforcement come in through many avenues, including rival sports bars that have legitimate program subscriptions. Agents who work for the major leagues or private investigators visit sports bars throughout the country to monitor what is being shown. Late last year, NFL Enterprises, Inc. filed civil suits against dozens of bars across the country for buying residential subscriptions to its NFL Sunday Ticket package. Residential subscriptions cost $139 for the football season, while commercial establishments pay from $600 to $2000, depending on their size.



A VCRS MODULE ready for insertion in a satellite-TV receiver. The smart-card slot provides for upgradable security.

To catch suspected signal pirates, NFL enterprises sent out teams of investigators to sports bars. During stops in play, the league caused all VideoCipher modules to display their identification numbers on the TV screen so that its investigators could note them and compare them against its subscription database.

Yet another form of satellite-signal theft occurs overseas. The Motion Picture Association of America (MPAA) has repeatedly cited the Caribbean area as a hotbed of piracy, both for pirated videocassettes and signal theft. However, the MPAA does not authorize cable programmers to distribute their services outside the U.S. If people in the Caribbean countries want cable services, they have no choice but to engage in signal theft.

"Technically, the footprint of the satellite signal is there," said Matthew Sappern, manager of corporate affairs for HBO. "HBO doesn't have the right to legally distribute and market its services outside the U.S. based on the covenants we have with the Hollywood studios." Because cable programmers lack distribution rights in the Caribbean area, their anti-piracy efforts are hindered.

According to Powers, the Caribbean Cable Association is lobbying the MPAA in Hollywood to allow the programmers to distribute outside the U.S. The MPAA has thus far not granted distribution rights because of its release schedule for new movies. The release schedule is a marketing umbrella whereby new movies are released first to the U.S. theaters, then to the foreign theater market, before being released for videocassette distribution, cable television and network television. This prevents a movie from appearing in the theaters and on videocassette or cable television at the same time.

Direct-broadcast satellites

In October of last year, a new satellite service was rolled out nationally: the RCA Digital Satellite System which broadcasts digital video and audio signals from high-power direct-broadcast satellites (DBS). The three major players responsible for the launch are RCA/Thomson Consumer Electronics, DirecTV (a unit of General Motors Hughes Electronics), and

United States Satellite Broadcasting (U.S.S.B, a division of Hubbard broadcasting).

The DSS rollout has been enormously successful so far, with RCA selling virtually all the hardware it can produce—100,000 units a month, according to the company. More than one million receivers could be sold before the service is one year old.

The encryption and conditional-access system chosen for DSS, a completely digital system, was developed by the News Datacom division of Rupert Murdoch's News Corporation. The receiver accepts a smart card through a slot in its front panel, which allows the receiver to decode the programming that it is authorized for.

The rationale for choosing the system is that the smart card is difficult to reverse-engineer, yet is easy and inexpensive to upgrade and replace if a security break makes it necessary. In that way, it is similar to VCRS.

However, in Europe, a very similar system from News Datacom provides conditional access control for the Sky satellite service. The system has been repeatedly subjected to "hacks" by satellite pirates. Officials of the companies involved remain confident that any security breaks in the DSS encryption will be repaired quickly and inexpensively.

What the law says

Signal theft became a Federal crime under the Cable Communications Policy Act of 1984 [Title 47 USC, Section 605]. The Act states that "No person shall intercept or receive or assist in intercepting or receiving any communications service offered over a cable system, unless specifically authorized to do so by a cable operator or as may otherwise be specifically authorized by law." Satellite-delivered programming, because it is distributed primarily to cable companies, is also covered under the Cable Act.

The Act clearly mentions equipment used for signal theft. It states: "For the purpose of this section, the term assisting in intercepting or receiving shall include the manufacture or distribution of equipment intended by the manufacturer or distributor (as the case may be) for unauthorized reception of any communications service offered over a cable system."

For a first offense under the Cable Television Consumer Protection and Competition Act of 1992 [Title 47 USC, Section 553], a fine of $50,000 and imprisonment of up to two years, or both, may be handed down. A repeat offender can be fined up to $100,000 and imprisoned for more than five years.

Only a manufacturer or distributor of illegal decoders or other descrambling devices is likely to receive imprisonment under the Cable Acts. A homeowner with no criminal record is not likely to go to jail for illegally connecting to the cable system. In many instances, the homeowner will be offered amnesty by the cable company and asked to subscribe.

"Our department performs many functions," says Bob Astarita, vice-president of security for Cablevision, the fifth largest Multiple Systems Operator (MSO) in the country. "One of the most critical is what we call a tap-audit function. Security technicians literally walk the system and make a determination if anyone is connected improperly or illegally."

In the first instance, according to Astarita, the illegal tap is treated as an unauthorized connection—one in which an individual is receiving programming through no fault of his own. That could happen, for example, if someone moved into an apartment and hooked his equipment up before determining that the prior occupant forgot to contact the cable company to have the service discontinued.

After the programming is cut off and the connection removed, a salesman will call and ask if the party would like to subscribe. If a tap audit discloses that the party is hooked up illegally a second time, it is treated as an illegal theft. The illegal connection is photographed and removed as evidence.

"Now you are illegal," says Henry Hack, director of investigations for Cablevision. "You have committed a crime. Theft of services is a Class A misdemeanor in New York State. You will be sent a cease-and-desist letter, and the security department will monitor the situation." No legal action will be

THE RCA DSS RECEIVER could be the next target for the concentrated efforts of pirates. The smart-card slot is located on the right side of the integrated receiver/descrambler or IRD.

taken unless the party hooks up for a second time. After the second offense, Cablevision will initiate either a civil action or a criminal action.

In a criminal action, a police officer will come to the house, determine that the party is hooked up illegally, and issue a desk appearance ticket. In New York State, theft of services is punishable by up to a $1000 fine or a year in jail. In most instances, if the homeowner has no criminal record, he will be able to plea bargain to a lesser offense. Most legal actions involve a civil suit. Damage awards start at about $1,500 in a civil suit.

"When I think of a pirate, I think of a seller or a distributor of illegal electronic products, not a homeowner," says Hack. "This is a business entity that advertises openly and is aware of the law." According to Hack, most illegal distributors do not sell in the states in which they are located to avoid prosecution under state law.

A typical brochure from a mail-order operation will display seemingly top-of-the-line equipment with brand names such as General Instrument, Panasonic, Toshiba and Scientific Atlanta. Usually, the channel converter, which can be legally acquired, will be offered for sale, along with the add-on or stand-alone descrambler—also called a starbase, a blackbox, a pancake, or a hotplate in the pirate trade.

In some instances, the equipment offered for sale is acquired from a cable operator who is about to upgrade the equipment in his franchise. In such cases, a distributor who buys the inventory that is to be upgraded diverts the equipment to a pirate operation.

"Piracy goes well beyond electronic hobbyists," Astarita said. "We encounter people who have Ph.D.s and others who have extensive backgrounds and degrees in many other academic disciplines."

Astarita, who is a former FBI agent, heads a staff of former law enforcement professionals. He and his staff conduct "buy-and-bust" operations and gather information to be used against pirate operations as part of their daily jobs.

THIS SPORTS BAR in New Jersey was sued for $1.4 million by Major League Baseball for showing out-of-town games without autorization.

Cable-signal theft can mean more than lost revenue to cable companies. One of the most serious problems caused by the proliferation of pirate electronic equipment is signal leakage. Hooking up an illegal decoder requires some technical expertise and the proper tools. A decoder that is not properly installed will cause signal leakage—radiation that poses a threat by interfering with commercial aircraft radio frequencies.

"We're supposed to be a closed system and there should be no leakage," said Hack. "The FCC does flyovers and measures the signal leakage, if the amount exceeds the cumulative leakage index (CLI), we will be fined heavily." Most cable operators have CLI teams who seek out potential signal leakage throughout the cable system.

Cable fights back

The technological battle between the cable companies and the pirates has led to some interesting anti-piracy devices, including the "electronic bullet." In April 1991, for example, American Cablevision of Queens, New York, filed suit against 317 cable customers who were pirating signals.

Jerrold Communications, a division of General Instrument Corp., learned that its converters were being compromised by an override chip. The black market chips were installed in a basic converter to obtain free premium programming. After obtaining several pirate devices, Jerrold engineers devised a strategy for outwitting the chip. The engineers invented a "bullet" that used the chip's own programs to neutralize it.

"The bullet is designed to blow out a box that has been tampered with," Hack explained. "Our computers talk directly to the decoders that we purchase from the manufacturer and tell it what to authorize. To use the bullet, we send a signal down the line that says: 'ignore the next message,' and the legitimate boxes will ignore the next message—the next

message being: 'blow yourself up.' There is no frying or electrical charge or 'bullet'—just a deauthorization." Incredibly, the bullet succeeded because irate homeowners with pirated boxes—unaware that a "bullet" had been fired—called the cable company to complain about the lack of reception.

Despite the penalties afforded under the Cable Acts of 1984 and 1992, the sale of illegal equipment is rampant. Illegal decoders are offered for sale in electronics stores, through mail-order companies, and are even advertised in national magazines. The sale and advertisement of illegal decoders can be found throughout the country.

Will Nix who joined the Motion Picture Association of America (MPAA) in 1976 and was promoted to the title of Chief Operating Officer of the MPAA's anti-piracy division, participated in organizing a nationwide effort to combat signal theft. Nix left the MPAA in 1991.

According to Nix, at one time during the 1980's about fifty percent of the satellite decoders sold by General Instrument were being compromised by a illegal computer chips. "General Instrument wanted to transfer its in-house anti-piracy effort into a larger, national effort," Nix said. "We helped organize the Office of Cable Signal Theft (OCST) as a joint effort by the Satellite Communications Broadcast Association (SCBA) and the MPAA."

OCST was formed in 1986 and today is part of the National Cable Television Association, in Washington, D.C., and funded by both the NCTA and the MPAA. OCST works closely with the Department of Justice, the F.B.I., U.S. Customs, state and local prosecutors, as well as law enforcement agencies throughout the country. OCST provides assistance to these enforcement agencies in prosecuting criminal violators. In the last three years, OCST has been involved in the seizure of 400,000 illegal decoders.

"Another organization that I assisted in forming is the Coalition Opposing Signal Theft (COST)," Nix said. "COST was set up as a joint venture between the NCTA and the MPAA, and was designed to address issues in the area of signal theft."

Many of the more than 10,000 cable operators are members in the OCST and COST, which is part of the OCST advisory committee. Mr. Astarita is the current vice-chairman of COST.

The inside problem

"When I first moved into Manhattan, the cable technician who hooked me up asked if I wanted to do this the legal way or the illegal way," said HBO's Matthew Sappern.

For some cash, the cable technician was offering to hook up the premium channels for Sappern, who would thereafter receive them for free. Sappern's experience is by no means an isolated one. Moreover, the largest source of illegal decoding devices on the black market today is cable operators themselves. It is estimated that as much as 90% of the market in illegal decoders can be traced back to the cable operators. It should be noted that in many instances, a cable operator who is upgrading his equipment will unknowingly sell his existing inventory to a distributor who, in turn, will divert the inventory to an illegal use.

"We at Cablevision are aware that a great deal of the illegal product comes from within," Astarita explained. "Cablevision monitors what happens to its old cable boxes, and in some instances we destroy the boxes if we cannot sell them to a reputable source."

Cablevision prides itself on being a leader in the field of addressing theft. It conducts due diligence inquiries on contractors and vendors with whom it does business. It will sell old cable products only to a distributor who can document the inventory's destination or to a licensed franchise cable operator.

Future problems?

Interactive television will dramatically change the content of cable programming and the problem of signal theft. In late 1994, Time Warner Cable Systems was scheduled to introducing interactive television to some 4000 homes in Orlando, Florida. The Orlando project will cost about $5000 per household. Digital Equipment Corp. and General Instrument Corp. are joining forces to produce the interactive equipment, which will combine DEC's microprocessor, distribution, and storage technologies with GI's encryption system that allows financial and other information to be sent confidentially.

The Orlando endeavor is the largest of many interactive television projects that will get underway this year. Interactive television will ultimately change the concept of the cable operator, who will be offering much more than simple television programming. EMInteractive television is the result of a merger of the technologies of many industries: computer, cable, television and telephone. Interactive television will allow the subscriber to 'interact' with the television. In the envisioned systems, the interactive cable subscriber will be able to talk face to face with his neighbor or his employer, shop and bank from his television, and view conventional television programming as well. Virtually all of the signals for interactive TV will be digital.

In June 1994, British television viewers got their first introduction to interactive television. Two commercial broadcasters, Carlton Television and London Weekend Television, joined forces with a cable operator to offer an experimental interactive London news channel. The cable operator's 65,000 subscribers can choose from four channels of programming to concentrate on weather, traffic, community and social action reports or the regular news program. In 1995, the cable operator hopes to introduce interactive programming that will allow the viewer to communicate with the studio. Viewers will be able to vote on programs or the performance of a politi-

Continued on page 90

VIDEO NEWS

continued from page 34

leave a message at the tone." Transmitted messages or pictures are automatically recorded on the Viewcam's Hi8 cassette, which permits up to two hours of audio or video information.

The system uses JPEG (Joint Photographic Experts Group) standards, has compression ratios of 20-, 15-, and 8-to-1, depending on the transmission speed; has a screen resolution of 384 × 240 pixels; and transmits images at 9600, 7200, 4800, and 2400 baud. Sharp thinks it will find many uses in business, where it's necessary to transmit detailed color images, as well as for personal use (sending baby pictures to Grandma, etc.).

The system isn't exactly cheap—the camcorder lists at $2500, the teleport at $900. And, of course, it takes two to tango. Ω

POWER CONTROLLER

continued from page 76

then turns it off. It then repeats that action for output 2, and so on. After output 7 toggles, the software then repeats the cycle.

Run and flash—This is a variation of the sequencer application. It sequences the outputs for five cycles, then flashes all eight three times and repeats the cycle.

Test—The test application tests the controller. The routine steps the outputs through all 32 power levels, pausing one second between each.

External—Here's where things get interesting. This routine allows an external source, such as an intelligent I/O module or a computer, to control power levels. To get into this mode, set switch S2 to a value of 2, install the correct jumpers, then reset the circuit. From then on, input Port C0 functions as a strobe that causes the microcontroller to read the value on Port A and perform the proper function.

When PC0 goes low, the microcontroller reads Port A. It then splits the value into a 5-bit power specification (PA0–PA4), and a 3-bit output port (PA5–PA7). The 5-bit power specification allows 1 of 32 values; the 3-bit output port allows 1 of 8 ports.

For example, assume you place the value $57 on Port A and strobe PC0 low. In binary, $57 = 0101 0111. Taking the upper three bits yields 010, or 2. Taking the lower 5 bits yields 10111, or 23. Thus the controller will set output 2 to level 23.

Summing up

As you can see, both hardware and software are simple and suitable for being customized. For example, you could connect the output of an A/D converter to Port A, then vary power levels based on some analog quantity.

When creating your own routines, be sure to include it in both the power-on Select routine and the Jump Table. That way the controller will know where to find it. Ω

SIGNAL THEFT

continued from page 40

cian and enter competitions.

By 1996, it is estimated that the U.S. market for digital cable converters will reach 4.5 million units annually, as cable companies upgrade the 65 million converter boxes now in use. The new converters—in conjunction with digital compression and fiberoptic cable—will expand the television's receiving capacity to perhaps as many as 500 channels.

Numerous joint ventures are underway to develop a new converter, and the result is that several types of converters will be on the market. Among the projects in progress: Hewlett-Packard is building a radio-based system. Intel, Microsoft, and General Instrument are creating a cable box based on Intel's microprocessors and GI's digital compression technology. Scientific Atlanta is building digital terminals for Time Warner's Full Service Network and U.S. West's video dialtone trial.

There is an industry-wide requirement for adequate signal security. A pirate who develops the technology to intercept a digitally compressed signal might be able to access a person's bank account, ATM number, and phone number, as well as other personal information.

The starting point for the scrambling that will be used for interactive television is the encryption already in use for digitally transmitted signals. Those transmitted signals are already in limited use by several programmers such as HBO.

Interactive television promises to be a revolution in television viewing. By any account it will be a boon to the cable industry and generally to the electronics industry. Reaping the full benefits of this technology will be no small feat. Signal theft will be one of the major obstacles. Not only will a foolproof encryption standard have to be developed, but intra-industry security must be carried out along with a uniform policy for marketing and distribution. Ω