


CRIMINAL COMPLAINT

UNITED STATES DISTRICT COURT		CENTRAL DISTRICT OF CALIFORNIA	
UNITED STATES OF AMERICA V. DENNIS MEGARRY		FILED CLERK, U.S. DISTRICT COURT FEB - 6 2003	Docket No. MAGISTRATE'S CASE NO. 03-0205M
CENTRAL DISTRICT OF CALIFORNIA BY DEPUTY			
Complaint for violation of Title 47, United States Code, § 605(e)(4)			
NAME OF MAGISTRATE JUDGE STEPHEN J. HILLMAN		UNITED STATES MAGISTRATE JUDGE	LOCATION Los Angeles, CA
DATE OF OFFENSE Unknown	PLACE OF OFFENSE Los Angeles County	Address of ACCUSED (IF KNOWN)	
COMPLAINANT'S STATEMENT OF FACTS CONSTITUTING THE OFFENSE OR VIOLATION: From a date unknown until on or about October 30, 2002, in Los Angeles County, within the Central District of California, and elsewhere, defendant Dennis Megarry distributed electronic, mechanical, or other devices or equipment, knowing or having reason to know that the devices or equipment were primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite service.			
BASIS OF COMPLAINANT'S CHARGE AGAINST THE ACCUSED: (See attached affidavit which is incorporated as part of this Complaint)			
MATERIAL WITNESSES IN RELATION TO THIS CHARGE:			
Being duly sworn, I declare that the foregoing is true and correct to the best of my knowledge.		SIGNATURE OF COMPLAINANT SCOTT WANAMAKER	
		OFFICIAL TITLE Special Agent - Federal Bureau of Investigation	
Sworn to before me and subscribed in my presence,			
SIGNATURE OF MAGISTRATE JUDGE(1) STEPHEN J. HILLMAN			DATE February 6, 2003

1) See Federal Rules of Criminal Procedure rules 3 and 54.
REC: DETENTION

JWS: 

SEARCH WARRANT AFFIDAVIT

I, Scott Wanamaker, being duly sworn hereby say and depose:

1. I am employed as a Special Agent ("SA") of the Federal Bureau of Investigation ("FBI") and have been so employed since September 29, 1998. I am assigned to the Los Angeles Field Office, Computer Intrusion Squad. Since April 1999, I have been assigned to investigate computer and high technology crimes. Before becoming a special agent, I was employed by the FBI as a Senior Computer Specialist for seven years and a Visual Investigative Analyst for two years. I have previously been assigned to investigate bank fraud allegations. I have received training from the FBI regarding computer crime, and have previously investigated computer crime violations and other violations employing various technologies. Additionally, I have a Bachelor of Science Degree in Information Systems.

2. I make this affidavit in support of a complaint and an arrest warrant charging Dennis Megarry ("Megarry") with violating Title 47, United States Code, Section 605(e)(4). This statute prohibits the manufacture and distribution of devices primarily of assistance in the unauthorized interception of satellite signal programming. For the reasons set forth below, there is probable cause to believe that Megarry has manufactured and distributed devices primarily of assistance in the unauthorized interception of satellite signal programming.

3. The facts set forth below are based upon my own personal observations, and upon reports and information provided to me by other law enforcement officers or individuals employed by or on behalf of DIRECTV, NDS Americas, Inc. (NDS), NagraStar L.L.C. (NagraStar) and EchoStar Satellite Corporation operating under the trade name DISH Network. I have not included in this affidavit all of the information I have uncovered relating to this investigation, but rather have set forth only such facts as I have deemed necessary to establish probable cause that Megarry has violated Title 47, United States Code, Section 605(e)(4).

TITLE 47, UNITED STATES CODE, SECTION 605(e)(4)

4. Title 47, United States Code, Section 605(e)(4) provides as follows: "Any person who manufactures, assembles, modifies, imports, exports, sells, or distributes any electronic, mechanical, or other device or equipment, knowing or having reason to know that the device or equipment is primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services, or is intended for any other activity prohibited by subsection (a) of this section, shall be fined not more than \$500,000 for each violation, or imprisoned for not more than 5 years for each violation, or both."

OVERVIEW OF OPERATION DECRYPT:

5. The Federal Bureau of Investigation began an undercover operation on December 20, 2001, known as Operation Decrypt, to infiltrate and prosecute members of the hacking communities dedicated to distributing hardware and software that is designed to circumvent the conditional access technologies of DirectTV and DISH Network. Operation Decrypt began in an effort to address an enterprise threatening theft problem in the entertainment industry. The entertainment industry, and other companies, are the victims of massive theft that, in the aggregate, results in billions of dollars of losses to the industry on an annual basis. One type of theft results from the hacking of conditional access smartcards used by DirectTV and DISH Network. As described below, the entertainment industry sells content to distributors, such as DirectTV and DISH Network, who in turn distribute that programming to consumers in exchange for a fee paid by the consumer to the distributor. The Federal Bureau of Investigation has infiltrated communities of smartcard hackers, and this case is one of many cases resulting from the Operation Decrypt undercover operation.

DESCRIPTION OF SATELLITE SIGNAL PROGRAMMING:

6. DirectTV, a California corporation, and EchoStar Satellite Corporation, a Colorado corporation, deliver digital entertainment and television programming to millions of homes and businesses in the United States. While DirectTV operates its

direct broadcast signal business under the name DirecTV, EchoStar operates its direct broadcast signal business under the trade name DISH Network. A consumer wishing to subscribe to DirecTV television programming or DISH network programming must first obtain necessary hardware items to receive the satellite signals. This hardware includes a satellite dish, an integrated receiver/decoder ("IRD"), and an access card or "smart card." The access card, or smart card, operates the IRD. Satellite programming currently includes major cable networks, major studio movies, special event programming offered on a pay-per-view basis, local channels, and a variety of other sports and special interest programs and packages.

7. NDS and NagraStar are developers and suppliers of proprietary encryption and smart card technology to DirecTV and DISH Network, respectively. The access card or smart card enables or authorizes the IRD to decrypt the encrypted transmissions from DirecTV or DISH Network satellites. The satellites, which are in geosynchronous orbit above the earth, relay encrypted signals to subscribers equipped with a dish and an IRD. The satellite signal is received by the dish and transmitted by wire to the IRD. The IRD contains a slot into which the access card is inserted, and the IRD processes the incoming signals.

8. An access card is provided to consumers along with the IRD. After a subscriber installs the dish and IRD at his or her home or business, and purchases one or more programming packages, the subscriber's access rights are electronically programmed on the access card by sending a signal through the satellite data stream to the subscriber's access card in the IRD. The access card contains computer chips with copyrighted software and acts as a re-programmable microprocessor using smart card technology to control the programming the subscriber can view based on the programming packages and programming purchased by the subscriber.

9. The access card is a key component in the security and integrity of the DirecTV or DISH Network satellite programming systems. To prevent unauthorized signal reception and program viewing, transmissions of television programming are encrypted at uplink facilities. The access card enables the subscriber's IRD to decrypt the signals and permits program viewing in accordance with the subscriber's authorized subscription package or pay-per-view purchases.

10. DirecTV and DISH Network has spent significant resources to protect the integrity of their satellite signals so that only authorized users are able to decrypt the programming. DirecTV and DISH Network combat theft by several means. One method employs electronic countermeasures (ECMs) that deny programming to illegally modified access cards. ECMs are

electronic messages sent through the satellite data stream to deactivate illegally modified access cards. Some of the ECMs "loop" the unauthorized software in the access cards to make the access cards inoperable. A community of unauthorized computer programmers and hardware manufacturers, which is sometimes referred to as the "pirate community" or the "smart card hacking community," is engaged in writing and distributing software on the Internet to circumvent these ECMs and develop hardware and software techniques to allow unauthorized users to obtain free satellite programming from DirectTV.

11. The pirate community is also actively engaged in manufacturing, distributing and selling unauthorized hardware devices that enable the unauthorized decryption of satellite signals. Such devices have limited or no legitimate commercial purpose other than to permit the illegal and unauthorized reception and decryption of encrypted television programming. One frequently used device that enables satellite signal theft is referred to as an "unlooper," and can restore the illegally modified software in a looped access cards to allow the card to intercept and decrypt satellite signals without authorization. The "unlooper" and other hardware devices, including "card loaders," "programmer/readers," "AVRs," "blockers," "emulators" and "computers," are all used to facilitate the unauthorized interception of satellite television signals. These hardware

devices are sometimes advertised on Internet web sites, in local publications, and in underground satellite publications.

12. To address the problem of unauthorized signal theft, in 1997 DirectTV introduced new access cards developed by its security vendor NDS to replace the original "first generation" access cards. New, supposedly secure second-generation cards, which are sometimes referred to as "Period 2" cards or "H" cards, were sent to all subscribers in 1997 to replace the first generation access cards. The pirate community developed ways to circumvent the H card by August 1997. The H Card is no longer manufactured and since August 2002 is no longer supported by DirectTV. In February 1999, DirectTV introduced a third generation access card, sometimes referred to as a "Period 3" card or an "HU" card. The first hack of the HU card was announced in November 2000 when a number of pirate Internet web sites advertised that they were selling illegally modified HU cards. Today, HU cards can be illegally programmed to intercept DirectTV's programming services.

13. In August 2002, DirectTV began distributing a fourth generation access card, known as the "P4" card or the "Period 4" card. The Period 4 card was the result of two years of development efforts by DirectTV and NDS and contains sophisticated proprietary technology of DirectTV never before used in any smart card application. DirectTV has invested more than \$25 Million to

develop the Period 4 access card. I have spoken to representatives from DirecTV, and to other agents participating in Operation Decrypt, who have confirmed that there are presently no known compromises of the Period 4 security features; the Period 4 access card is presently secure, although numerous Internet websites (most of which are hosted outside the United States) post information and techniques to support those attempting to develop ways to circumvent the security features of the Period 4 card.

14. Currently, there are several hundred web sites devoted to selling pirate hardware and software. The pirate hardware and software is used to modify Period 3 and previously Period 2 DirecTV access cards to unlawfully receive programming services without authorization ("pirate community websites"). These sites are also devoted to circumventing DISH Network conditional access cards. DirecTV has recently replaced the Period 2 access cards with Period 4 access cards, but the Period 3 access card is used by the majority of DirecTV customers to receive DirecTV programming.

PROBABLE CAUSE:

15. On August 3, 2002, a search warrant was executed at the residence of an individual herein referred to as "Confidential Source" or "CS-2." Numerous modified DirecTV access cards and

various hardware devices used for the unauthorized interception of satellite signals were seized during this search.

16. On August 3, 2002, CS-2, who resides and works in Los Angeles County, within the Central District of California, was interviewed by FBI SA Christopher E. Beausang of the Los Angeles Field Office and provided the following information:

a. CS-2 advised Agent Beausang that he was involved in the pirating of DirectTV by building and selling hardware devices used for the unauthorized interception of television satellite signals. More specifically, CS-2 explained that he constructed HU loaders and unloopers by reverse engineering the devices.

b. Based on these reverse engineering efforts, CS-2 purchased printed circuit boards, added the necessary parts, such as the Atmel computer chip, and then programmed or "flashed" the chips to permit the unauthorized interception of satellite signals.

c. As part of these piracy efforts, CS-2 purchased circuit boards with an individual known to CS-2 as Dennis Megarry.

d. CS-2 communicated on the Internet with Megarry who ran a Website named www.baracudatec.com, and also telephonically communicated with Megarry at cellular telephone number (740) 703-0580.

e. In the Spring of 2001, CS-2 showed Megarry an "HU" loader schematic design and Megarry found a company in Lake Forest, California, willing to assemble printed circuit boards using that schematic design. (As discussed above, the "HU" access card is DirectTV's Period 3 access card.)

f. Megarry placed large orders with the company and included with his orders smaller orders for CS-2.

g. Megarry's contact at the Lake Forest, California company was an individual named "Greg" (last name unknown), who CS-2 described as a "major circuit board distributor."

h. CS-2 and Megarry also purchased from the same company in Lake Forest, California, ISO programmers, which as discussed above are devices used to program DirectTV cards to permit the unauthorized decryption of satellite signal programming.

i. Megarry also purchased HU loaders that were produced by the same company that manufactured the circuit boards located in Lake Forest, California. These HU loaders, which Megarry subsequently sold, were cloned from a loader called "MONGOOSE," and had a different design logo than did the ones purchased by CS-2.

j. CS-2 built between 300 to 350 HU loaders and sold them for about \$50 to \$75 per board, and the HU loaders were

sold for the purpose of unauthorized decryption of satellite signal programming.

k. CS-2 paid Megarry via PayPal, an online Internet payment service, or through money orders, for his portion of the orders that accompanied Megarry's larger orders.

l. Megarry's PayPal account was paypal@baracudatec.com, and Megarry had a mailing address of 90 Taylor Road, Waverly, OH 45690.

17. On September 27, 2002, Special Agents with the FBI directed CS-2 to telephone Megarry at (740)703-0580. This telephone call was consensually recorded and FBI SA Tracy Kierce of the Los Angeles Field Office reviewed the recording and informed me of the following:

a. Megarry answered the telephone and acknowledged that he was at his residence and had received an e-mail from CS-2.

b. Megarry told CS-2 that he had moved to a new house during the last weekend, that he (Megarry) still owned an airplane, and that the airport was four and one-half miles from his new house, which was situated on 200 acres.

c. Megarry said that he was buying the "Mikobu II," with a case, for \$35 each from an individual in Texas, and further stated that he had only five on hand which were "going out," but stated that he was getting ready to place

another order and that if he and CS-2 ordered "a hundred" they could probably get them cheaper.

d. CS-2 asked Megarry about the "Mikobu" device and inquired "does it do like DISH and everything too or just DirectTV?" Megarry said words to the effect that he was not sure, but that it was supposed to do "everything" and that it did not look much different than the regular "Mikobu."

e. CS-2 told Megarry that he (CS-2) would need to get some of the devices since he had some people requesting loaders. Megarry responded that he was sending individuals the "Mikobu" instead of a "glitcher," and no one had complained. (Like the Mikobu, the glitcher is also a hardware device primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services.)

f. Megarry also said that he had "one guy" buying a whole bunch of the unlooper boards from him, and that he (Megarry) had 500 circuit boards and AVR boards on hand. CS-2 inquired about "Greg" and Megarry said that Greg had not obtained the devices Megarry had requested.

g. Megarry told CS-2 that he would be placing an order for the "Mikobus" next week, and CS-2 said that he would let Megarry know what he (CS-2) wanted to order.

18. On October 1, 2002, at the direction of the FBI, CS-2 telephoned Megarry at (740) 703-0580 and the telephone call was consensually tape recorded. I listened to the tape recording of this call and determined that an individual identifying himself as Megarry answered the telephone, and that CS-2 said he needed 25 "Mikobu" loaders and 25 AVR4s.

19. On October 3, 2002 at 1:07 p.m., CS-2 sent an e-mail to Megarry at email address dennis@megarry.com, and received an e-mail response from Megarry on October 3, 2002 at approximately 2:28 p.m. PDT. The e-mail exchange included the following:

a. The message sent to Megarry by CS-2 read as follows: "Hey Dennis, I need 25 of the AVR 4's @\$15.00 each. Give me the total with shipping and the addy to send the payment to? Thanks."

b. The response from Dennis Megarry to CS-2 read as follows: "Depends on how you want it shipped . . \$25 should cover expenses . . \$13 for Priority... Send to: Dennis Megarry 5600 S.W. US 42, Ostrander, OH 43061."

20. On October 7, 2002, I purchased a United States Postal Money Order, serial number 04622327493, ("United States Postal Money Order") in the amount of \$388 to provide to CS-2 to cover the purchase of the 25 AVRs, plus shipping costs.

21. On October 07, 2002, FBI Special Agent Jeffrey Cugno, who is also participating in Operation Decrypt, provided the

United States Postal Money Order to CS-2. The next day, October 8, 2002, CS-2 told SA Cugno that he had mailed the United States Postal Money Order to Megarry at "5600 US Highway 42, Ostrander, OH 43061."

22. After the e-mail exchange between Megarry and CS-2 on October 3, 2002, SA Kierce conducted follow-up investigation relating to the information from the e-mails described above, as well as information relating to the tape-recorded telephone conversations between CS-2 and Megarry. Through this follow-up investigation SA Kierce informed me that she learned the following information:

a. On October 19, 2002, SA Kierce reviewed the extended header information in connection with the October 3, 2002, e-mail response from Megarry to CS-2, and determined that the e-mail had been sent from Internet Protocol (IP) address 65.24.50.9. SA Kierce then reviewed a report from Christine A. Dzujna, Administrator, Legal Affairs, Time Warner Roadrunner Cable, and ascertained the following subscriber information relating to IP address 65.24.50.9 on October 3, 2002 at 2:28 p.m.:

i. The subscriber is Dennis Megarry at address of 5600 US Highway 42, Ostrander, OH 43061, telephone number (740) 703-0580.

ii. The account was installed on September 25, 2002.

b. On October 19, 2002, SA Kierce reviewed a report concerning telephone number (740) 881-5389 from Verizon North, Verizon Legal Compliance and determined that the subscriber on the account is Dennis Megarry at the address of "5600 US Route 42 S. Delaware, OH 43015." SA Kierce also reviewed a report prepared by me and determined that Verizon North had advised SA Wanamaker that the address 5600 US Route 42 S., Delaware, OH is where the telephone line terminates.

c. On October 19, 2002, SA Kierce reviewed a search of public records conducted on October 15, 2002 and determined that "Dennis W. Megarry" had a current address listed of 5600 US Highway 42, Ostrander, Ohio 43061, and that "Dennis Megarry" is a certified private pilot.

d. On October 20, 2002, in an effort to corroborate Megarry's statements to CS-2 during their recorded telephone conversation on September 27, 2002, relating to the proximity of the airport to his house, SA Kierce determined through Internet website www.mapquest.com that the driving distance from the Delaware Municipal Airport located at 1075 Pittsburgh Drive, Delaware, Ohio to 5600 Highway 42, Ostrander, Ohio, is 5.74 miles.

e. On October 21, 2002, SA Kierce telephonically contacted Jeremy Roybal, PayPal, which is an Internet payment service, and determined that Megarry has been restricted from accessing his PayPal account since September 19, 2002. For the period from January 29, 2000, when the account was opened, to October 21, 2002, Megarry had received a total of approximately \$133,587 in payments.

f. On October 21, 2002, SA Kierce reviewed the PayPal records of CS-2 and determined that on July 17, 2001, Megarry sent payment of \$166 to CS-2 for the purchase of a "Mongoose" from Dennis Megarry's PayPal account: paypal@baracudatec.com. The note from Megarry to CS-2 read as follows: "If you ship via USPS Express Mail, they will deliver on Sunday even at no extra charge!"

g. On October 21, 2002, SA Kierce reviewed the PayPal records of CS-2 and determined that on July 25, 2001, Megarry sent payment of \$521 to CS-2 for the purchase of 100 JT-Tek Unlooper PCBs.

h. On October 22, 2002, SA Kierce reviewed a letter from the United States Postal Service Police that advised "Dennis Megarry-Wadsworth" submitted a change of address as of October 1, 2002, and a forwarding address of 5600 US Highway 42, Ostrander, Ohio 43061. The former address for "Dennis Megarry" was 90 Taylor Road, Waverly, Ohio 45690.

i. On October 22, 2002, SA Kierce contacted Russell Densmore, Manager, DISH Network Signal Integrity, Echostar Technologies, concerning the hardware device known as an AVR or audio video replicator. Densmore advised that he knows of no other purpose for an AVR other than to circumvent DISH Network conditional access technologies. The AVR's only known purpose is the theft of satellite signals. The "8515" chip is the Atmel chip, AT 90S-8515.

23. On or about October 21, 2002, CS-2 advised SA Cugno that Megarry had confirmed to CS-2 that he (Megarry) received the United States Postal Money Order and would be sending the AVRs to CS-2.

24. On October 23, 2002, SA Cugno informed FBI SA Christopher Beausang that CS-2 had provided him (SA Cugno) with the consensually monitored telephone conversations between CS-2 and Megarry, and SA Cugno gave the tape to SA Beausang who listened to the tape and learned the following:

a. On October 23, 2002, CS-2 telephoned Megarry at 740-703-0580 at 12:32 p.m. (PDT), and in this conversation Megarry told CS-2 said that he (Megarry) had sent the AVR boards to CS-2 the previous day via UPS, and that CS-2 should receive the package before noon.

b. Megarry told CS-2 the address to which he had sent the package and said that the package tracking number was EU337602395US.

25. On October 23, 2002, SA Cugno received one UPS package from CS-2, which CS-2 had received in the Central District of California on October 23, 2002. SA Beausang examined the package and determined that the package mailing label showed the sender as Barracuda Tech, 5600 S.W. US 42, Ostrander, OH 43061. The label further showed that the package had been sent date on October 22, 2002. The package tracking number was EU337602395US. FBI SA Jason N. Smolanoff and SA Beausang opened the package and found that it contained twenty-five AVR boards.

26. On October 30, 2002, Megarry's residence was searched as part of a coordinated search sweep of the residences of 16 individuals located in eight states suspected of engaging in satellite signal piracy. The search of Megarry's residence was conducted by FBI SAs located in the Columbus, Ohio Field Office. During the search of Megarry's residence, the following items, among others, were recovered that indicate to me, based upon my training and experience, that Megarry sold and distributed devices that are primarily of assistance in the unauthorized decryption of satellite cable programming, or direct-to-home satellite services:

- a. Nineteen conditional access cards for satellite cable programming service;
- b. A "Barracuda Unlooper" with a Priority Mail envelope;
- c. A box of Barracuda Smart Cards;
- d. A box containing unassembled AVR boards and unassembled unlooper boards;
- e. Numerous program boards and resistors; and
- f. A Federal Express box containing unassembled loaders.

27. On or about January 29, 2003, I consulted with experts in the signal integrity and engineering offices of DirecTV and learned that a sample of the seized conditional access cards that I had delivered to DirecTV for analysis included nine cloned access cards and other conditional access cards that were similarly modified unlawfully.

I declare under penalty of perjury that the foregoing is true and correct.

151

Scott Wanamaker
Special Agent
Federal Bureau of Investigation
Los Angeles, California

Sworn and subscribed to before
me this 6th day of February, 2003.

STEPHEN J. HILLMAN

STEPHEN J. HILLMAN
UNITED STATE MAGISTRATE JUDGE