FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff-Appellee,* v. PETER THOMAS HARRELL, *Defendant-Appellant.*	No. 07-10238 D.C. No. CR-05-00475-LKK OPINION

Appeal from the United States District Court
for the Eastern District of California
Lawrence K. Karlton, Senior Judge, Presiding

Argued and Submitted
March 11, 2008—San Francisco, California

Filed June 30, 2008

Before: Stephen Reinhardt, Melvin Brunetti, and
Raymond C. Fisher, Circuit Judges.

Opinion by Judge Brunetti

COUNSEL

Daniel J. Broderick, Federal Defender, Sacramento, California, for the defendant-appellant.

McGregor W. Scott, United States Attorney, Sean C. Flynn, Assistant United States Attorney, Sacramento, California, for the plaintiff-appellee.

OPINION

BRUNETTI, Circuit Judge:

Peter Thomas Harrell (Harrell) appeals in part the district court's partial denial of his motion for return of property filed pursuant to Federal Rule of Criminal Procedure 41(g). Acting pursuant to a warrant, officers seized the property at issue from Harrell's residence in 2004. A federal indictment followed, but was dismissed after the district court granted Harrell's suppression motion. Harrell now seeks the return of some property still in the government's possession.

I. Facts and Proceedings

DISH Network and Direct TV are direct broadcast satellite services that broadcast encoded digital satellite television and audio signals throughout the United States. To obtain either service, subscribers must purchase or lease equipment, including receivers, which decode and convert the encoded satellite signal into a viewable television signal, and "smartcards," which authorize the receiver to convert the signal. Each DISH Network receiver has a unique "boxkey" identification number which is electronically stored in the receiver and is used by DISH Network to identify the receiver and to obtain information about the receiver. While boxkey identification numbers are proprietary and are generally not made available to the public, they may be obtained using a receiver's J-TAG port, which is the input/output port used to interface the receiver with a personal computer for reading and writing receiver software.

On October 27, 2004, acting pursuant to a warrant, officers of the Siskiyou County Sheriff's Department seized various items of personal property from Harrell's residence. The property included satellite television receivers, smartcards, and other related electronics, compact discs, computers and hard drives. The sheriff's department turned the property over

to the Signal Integrity Division of EchoStar Technologies Corporation (doing business as DISH Network) for inspection and analysis. Between November 2004 and February 2005, Michael J. Clifford (Clifford) inspected and analyzed the property to establish whether the seized receivers and smartcards were modified to receive unauthorized programming. Clifford concluded that fourteen of the twenty-seven seized receivers were "modified to receive unauthorized satellite programming." Another twelve receivers were either unmodified, could not be used to pirate a signal, or were not analyzed. The one remaining receiver belonged to Richard Harding, not Harrell, and Harrell does not seek its return.

The fourteen receivers Clifford found to be "modified to receive unauthorized satellite programming" fall into four subcategories:

1. receivers with what appears to be their boxkey identification numbers written on their bottoms in black magic marker;

2. receivers with their boxkey identification numbers written on their bottoms in black magic marker, and scratches, marks and mars on their J-TAG ports, which is consistent with using a J-TAG interface device to extract a boxkey identification number;

3. receivers with their boxkey identification numbers written on their bottoms in black magic marker, and scratches, marks and mars on their J-TAG ports, and a history of unauthorized use; and

4. one receiver with only scratches, marks and mars on its J-TAG port.

Clifford also issued reports on the seized smartcards, computer hard drives, and other miscellaneous items. These miscellaneous items include:

1. digital locks (used to evade electronic countermeasures sent by satellite service providers to combat piracy);

2. satellite finders (used to identify locations with optimum signal reception);

3. J-TAG interface devices (used to transfer software between receivers and personal computers);

4. Sombreros (used to extract boxkey identification numbers from receivers);

5. memory erasers (used to erase smartcard memories);

6. ATMEGA 128 devices (used in lieu of smartcards to pirate satellite signals); and

7. audio-video replicator programmers (used to load piracy software onto various piracy devices).

Finally, Clifford issued reports on software downloads for piracy devices, instructions on how to use piracy devices, instructions on the piracy of DISH Network smartcards, instructions on the installation of digital locks, and instructions on the extraction of boxkey identification numbers.

The Siskiyou County Sheriff's Department assigned numbers to each item of seized property, which are reflected in its Department Evidence Report (e.g., 001CS, 001SW, 002CS, etc.). When an item number encompassed multiple items of

property, Clifford then assigned items or groups of items different item numbers, which are reflected in his analysis reports (e.g., 24E, 24G, 24I, etc.). Throughout the district court proceedings, the parties referred to items by the item numbers assigned to them in the Department Evidence Report, and when possible we do the same. However, because Harrell also refers to specific items by Clifford's item numbers, we use those identifying numbers as well, when necessary.

After the Siskiyou County Sheriff's Department transferred Harrell's property to the FBI, a grand jury returned a four-count indictment against Harrell, charging various violations of 18 U.S.C. § 1029 and seeking criminal forfeiture of the seized property.[1] After the district court granted Harrell's motion to suppress the seized evidence, the court granted the government's motion to dismiss the indictment without prejudice.

---

[1]Section 1029 states, in pertinent part:

> (a) Whoever—
>
> . . .
>
> (7) knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services;
>
> . . .
>
> (9) knowingly uses, produces, traffics in, has control or custody of, or possesses hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization;
>
> . . .
>
> shall, if the offense affects interstate or foreign commerce, be punished as provided in subsection (c) of this section.

Harrell then filed the instant motion pursuant to Federal Rule of Criminal Procedure 41(g), seeking return of the property seized from his residence.[2] Harrell's motion included as exhibits the Siskiyou Sheriff's Department Evidence Report and all of Clifford's reports. In his motion, Harrell states that he does not seek the return of any property modified to permit the owner to illegally view encrypted television signals, nor does he seek the return of any discs with downloaded instructions explaining how to modify equipment to permit the illegal viewing of encrypted television signals.

In response, the government filed two declarations from Donald Toy (Toy), Clifford's supervisor and the manager of the Signal Integrity Division, which inspected and analyzed the seized property. The government supported its response with Toy's declarations because at the time Harrell filed his Rule 41(g) motion, Clifford was no longer employed by DISH Network. Toy concluded that the DISH Network receivers and smartcards in Harrell's possession were "modified to receive unauthorized programming," and that Harrell also possessed pirating hardware and software.

The parties stipulated to submit Harrell's motion on the papers, and Harrell waived any objection to the government's reliance on Toy's declarations. After noting that the "parties agree that certain property should be returned to [Harrell]," the court specifically discussed the receivers contested by the parties. The court stated:

---

[2]Rule 41 states, in pertinent part:

> (g) Motion to Return Property. A person aggrieved by an unlawful search and seizure of property or by the deprivation of property may move for the property's return. The motion must be filed in the district where the property was seized. The court must receive evidence on any factual issue necessary to decide the motion. If it grants the motion, the court must return the property to the movant, but may impose reasonable conditions to protect access to the property and its use in later proceedings.

> Mr. Toy based his opinion on the fact that the box-keys of the receivers were written on the bottom of the units, there was [sic] scratches and marks on the J-TAG ports of the receivers, and "information from the nonvolatile memories indicate that [the] receivers have been receiving authorized programming." . . . Given that [Harrell] does not object to Mr. Toy's declaration, the court accepts Mr. Toy's conclusion that the receivers have been illegally modified and are capable of receiving unauthorized programing.

No. CR. S-05-475 LKK, 2007 WL 1279505, at * 2 (E.D. Cal. May 1, 2007) (second alteration in original). Therefore, the court concluded, the contested receivers constitute contraband per se under section 1029(a)(7). The court then discussed the miscellaneous seized items. Other than certain cables and adaptors, which the government agrees to return, the court again accepted Toy's conclusions as fact, construed items 020SW and 021SW as capable of pirating and/or having been illegally altered, and found that they should not be returned to Harrell. In sum, the court ordered:

> [Harrell's] Motion for Return of Property is granted in part and denied in part. The government shall return to [Harrell] the following items: blue cards (item # 032SW), hard drives (item # s 002CS & 003CS), remote control (item # 10SW), unmodified receivers (item # s 013SW, 014SW, 025SW-031SW), paperwork (item # 018SW)[,] computer (item # 034SW), and various cables and adaptors associated with items # 020SW and # 022SW. The government shall retain the remainder of the property in question.

Id. at *3. This appeal followed.

II. Standards of Review

We review the denial of a motion for return of property de novo. *United States v. Kaczynski*, 416 F.3d 971, 974 (9th Cir.

2005). We review the district court's factual findings for clear error. *United States v. Marolf*, 173 F.3d 1213, 1216 (9th Cir. 1999).

III. Discussion

[1] "When a motion for return of property is made before an indictment is filed (but a criminal investigation is pending), the movant bears the burden of proving both that the seizure was illegal and that he or she is entitled to lawful possession of the property." *United States v. Martinson*, 809 F.2d 1364, 1369 (9th Cir. 1987) (citations omitted). "However, when the property in question is no longer needed for evidentiary purposes, either because trial is complete, the defendant has pleaded guilty, or . . . the government has abandoned its investigation, the burden of proof changes. The person from whom the property is seized is presumed to have a right to its return, and the government has the burden of demonstrating that it has a legitimate reason to retain the property." *Id.* (footnotes and citations omitted). The "government must justify its continued possession of the property by demonstrating that it is contraband or subject to forfeiture." *Id.* (citations omitted). Here, the government argues that all of the property Harrell seeks to have returned is contraband per se.

[2] An object is contraband per se if its possession, without more, constitutes a crime; or in other words, if there is no legal purpose to which the object could be put. *United States v. McCormick*, 502 F.2d 281, 288 (9th Cir. 1974); *see also United States v. Bolar*, 569 F.2d 1071, 1072 (9th Cir. 1978) (per curiam) (explaining that while diamond rings are not contraband per se, negatives of Federal Reserve Notes are). The government argues that the seized receivers are contraband per se under section 1029(a)(7), and that the seized smartcards, programming electronics, and other pirating hardware and software are contraband per se under section 1029(a)(9).

A. Receivers

[3] Section 1029(a)(7) imposes penalties on any person who "knowingly and with intent to defraud uses, produces, traffics in, has control or custody of, or possesses a telecommunications instrument that has been modified or altered to obtain unauthorized use of telecommunications services." The government argues that receivers 001SW, 002SW, 003SW, 004SW, 005SW, 006SW, 007SW, 008SW, 009SW, 011SW, 012SW, 015SW, 016SW, and 017SW "are nothing if they have not been 'modified or altered to obtain unauthorized use of telecommunications services.' "

[4] As noted, these fourteen receivers fall into four subcategories:

1. four receivers with what appears to be their respective boxkey identification numbers written on their bottoms in black magic marker (011SW, 012SW, 015SW, 017SW);

2. seven receivers with their respective boxkey identification numbers written on their bottoms in black magic marker, and also, scratches, marks and mars on their J-TAG ports (002SW, 004SW, 005SW, 006SW, 007SW, 008SW, 016SW);

3. two receivers with their boxkey identification numbers written on their bottoms in black magic marker, and scratches, marks and mars on their J-TAG ports, and a history of past unauthorized use (001SW, 003SW); and

4. one receiver with only scratches, marks and mars on its J-TAG port (009SW).

In this case, whether any of these receivers are contraband per se depends upon whether they are "modified or altered to

obtain unauthorized use of telecommunications services" under section 1029(a)(7). Whether these receivers could be contraband per se under another statutory provision is not before us.

[5] Section 1029 does not explicitly define "modified or altered"; therefore, we interpret those words to have their ordinary meaning. *Emmert Indus. Corp. v. Artisan Assocs., Inc.*, 497 F.3d 982, 987 (9th Cir. 2007) (explaining that "unless statutory terms are otherwise defined, they are generally interpreted in accordance with their ordinary meaning" (internal quotation marks omitted)). *Black's Law Dictionary* defines a modification as a "change to something; an alteration." 1025 (8th ed. 2004). Similarly, a lay dictionary defines modify as to "make partial changes in; make different"; and defines alter as to "make or become different; change." *Oxford American Dictionary of Current English* (1st ed. 1999). Giving modified and altered their ordinary meanings, we conclude that there must be a change to either the hardware or software of a telecommunications instrument that makes it more capable of obtaining unauthorized signals in order for it to be "modified or altered" under section 1029(a)(7). *See, e.g.*, *United States v. Mendez-Carrero*, 196 F. Supp. 2d 138, 140 (D. P.R. 2002) (explaining that section 1029(a)(7) applies to cellular phones with reprogrammed microchips and cellular phones programmed to emit random Electronic Serial Numbers-Mobile Identification Numbers both of which allow calls to be made without being billed); *United States v. Alvelo-Ramos*, 957 F. Supp. 18, 18-19 (D. P.R. 1997) (explaining that cloned cellular phones fall within the ambit of section 1029). The government cites no legislative history or cases warranting a more expansive reading of "modified or altered," the district court did not discuss any, and we have found none.[3]

[3]Because we are construing a criminal statute, we also apply the rule of lenity, which favors a narrow construction of ambiguous terms. *See*

In addition to giving modified and altered their ordinary meaning, our reading of section 1029(a)(7) is consistent with other cases in which the government sought to combat the unauthorized viewing of satellite television under other statutory provisions, namely 18 U.S.C. § 2512 and 47 U.S.C. § 605(e)(4).[4] In *United States v. Lande*, we held that the Elec-

Fernandez-Ruiz v. Gonzales, 466 F.3d 1121, 1127 (9th Cir. 2006) (en banc) (noting that courts should apply the rule of lenity when interpreting criminal statutes "in both criminal and noncriminal cases," and therefore "courts should construe . . . ambiguous statutory language against the government").

[4]Section 2512 states, in pertinent part:

> (1) Except as otherwise specifically provided in this chapter, any person who intentionally—
>
> . . .
>
> (b) manufactures, assembles, possesses, or sells any electronic, mechanical, or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of wire, oral, or electronic communications, and that such device or any component thereof has been or will be sent through the mail or transported in interstate or foreign commerce;
>
> . . .
>
> shall be fined under this title or imprisoned not more than five years, or both.

Section 605 states, in pertinent part:

> (e) Penalties; civil actions; remedies; attorney's fees and costs; computation of damages; regulation by State and local authorities
>
> . . . .
>
> (4) 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

tronic Communications Privacy Act, 18 U.S.C. §§ 2510-2521, prohibits the modification of descramblers to allow unauthorized viewing of scrambled satellite television. 968 F.2d 907, 908 (9th Cir. 1992). We specifically noted that "Lande modified the . . . satellite descrambler module by copying the electronic 'address' of a subscriber's . . . unit on blank computer chips, which he then installed in other . . . descramblers," and that "Lande then added a new computer chip to the . . . units so the modified descramblers would unscramble all stations." *Id.* at 908-09. In *United States v. Harrell*, 983 F.2d 36, 37 (5th Cir. 1993), where the government alleged violations of both section 2512(1)(b) and section 605(e)(4), the court noted that the modules at issue "had been implanted with a chip . . . in order that non-paying usurpers could unscramble encrypted satellite transmissions." Finally, in *United States v. Shriver*, the court explained that "descramblers are modified by removing and replacing [their] unique address with a 'working address,' an address identical to that of another descrambler, the latter of which is programmed to descramble a greater number of encrypted programs." 989 F.2d 898, 900 (7th Cir. 1992). Each of these cases involves changes to either the hardware or software of descramblers.

[6] Here, the only change to receivers 011SW, 012SW, 015SW and 017SW is that they each have what appears to be their respective boxkey identification numbers written on their bottoms in black magic marker. However, because writing a series of numbers on a receiver in black magic marker is neither a change to hardware nor software that makes the receiver more capable of obtaining unauthorized signals, these four receivers are not "modified or altered," and are therefore not contraband per se under section 1029(a)(7).

$500,000 for each violation, or imprisoned for not more than 5 years for each violation, or both. For purposes of all penalties and remedies established for violations of this paragraph, the prohibited activity established herein as it applies to each such device shall be deemed a separate violation.

[7] In addition to having their respective boxkey identification numbers written on their bottoms in black magic marker, receivers 002SW, 004SW, 005SW, 006SW, 007SW, 008SW, and 016SW also have scratches, marks and mars on their J-TAG ports. Again, however, there is no evidence that these scratches, marks or mars change either the hardware or software of these receivers. Therefore, the government did not bear its burden of showing these receivers to be "modified or altered," and they too are not contraband per se. Similarly, receiver 009SW is not contraband per se because it only has scratches, marks and mars on its J-TAG port.

[8] Receivers 001SW and 003SW present somewhat of a closer question because their non-volatile memories indicate past receipt of unauthorized satellite programming.[5] In the end, however, our conclusion is the same. As the government acknowledges, smartcards control the level of programming accessible by a given receiver, not the receiver itself. Therefore, despite the fact that these two receivers' non-volatile memories indicate past receipt of unauthorized programming, that does not necessarily mean they are "modified or altered" under section 1029(a)(7). A "modified or altered" smartcard could have allowed receipt of unauthorized programming without any change to the receivers' hardware or software, and the government has not otherwise shown that these receivers, in and of themselves, are "modified or altered to obtain unauthorized use of telecommunications services." Unlike in the cases discussed above, there is no evidence of computer chips having been added to these two receivers, nor is there evidence that the receivers' software has been changed in any way. Furthermore, the apparent addition of solder to receiver 001SW's J-TAG port, without more, does not establish a modification or alteration to obtain unauthorized telecommunications services. Therefore, the government

[5]Non-volatile memory is computer memory that can retain stored information even when not powered.

did not satisfy its burden of establishing receivers 001SW and 003SW as contraband per se.

We note that the district court ordered the government to return nine unmodified receivers to Harrell (013SW, 014SW, 025SW, 026SW, 027SW, 028SW, 029SW, 030SW, 031SW). The government now concedes that Harrell is also entitled to the return of two additional receivers (019SW, 024SW). Receiver 019SW is not contraband per se because Clifford concluded that it "has not been modified," and receiver 024SW is not contraband per se because Clifford concluded that "[i]t was produced for the Asian market," and that "it is not possible to capture a DISH Network satellite television signal" with it. Finally, receiver 023SW must be returned to Harrell because Toy concluded that it is unmodified, and the government did not seek to retain it in its response. To the extent the district court concluded that receivers 019SW, 023SW and 024SW have been changed in any way, those factual findings are clearly erroneous, and the receivers must be returned to Harrell.

To recap our analysis, with respect to the seized receivers, the government must return the following twenty-six receivers to Harrell because the government does not seek to retain them, or the government did not show them to be modified or altered to obtain unauthorized use of telecommunications services under section 1029(a)(7), or they cannot capture a DISH Network satellite television signal: 001SW, 002SW, 003SW, 004SW, 005SW, 006SW, 007SW, 008SW, 009SW, 011SW, 012SW, 013SW, 014SW, 015SW, 016SW, 017SW, 019SW, 023SW, 024SW, 025SW, 026SW, 027SW, 028SW, 029SW, 030SW and 031SW. The government may retain possession of receiver 004CS because Harrell does not seek its return.

B. Smartcards, programming electronics, and other hardware and software

The government next argues that smartcards, programming electronics, and other seized hardware and software are con-

traband per se under section 1029(a)(9) and should not be returned to Harrell. Section 1029(a)(9) makes it a crime to "knowingly . . . [possess] hardware or software, knowing it has been configured to insert or modify telecommunication identifying information associated with or contained in a telecommunications instrument so that such instrument may be used to obtain telecommunications service without authorization . . . ."

Specifically, the government argues that possession of the property encompassed in items 020SW, 021SW and 022SW is in and of itself a crime and that the district court properly determined that the property should not be returned to Harrell. After again accepting Toy's conclusions as fact, the court "construe[d] items 020SW and 021SW as capable of pirating and/or having been illegally altered," and found that they should not be returned to Harrell. *See* 2007 WL 1279505, at *2. The district court did not separately address item 022SW. In reaching its conclusion, the court specifically noted that Harrell "does not seek to have returned to him any items which are capable of pirating." *Id.* There is some support for the district court's assertion in the record; in Harrell's initial motion he states that he has no desire to have property encompassed within items 020SW and 022SW returned to him that "are identified as having no 'legitimate' use, piracy devices, or used in the pirate community." However, in his reply, Harrell clarified that unless an item "is accompanied by a reliable explanation that it has no known legitimate purpose, it must be returned" to him. Harrell argues that items 020SW and 022SW must be returned to him because the government did not satisfy its burden of showing these items to be contraband per se.

The Department Evidence Report describes item 020SW as including miscellaneous "smartcard programming electronics," and item 022SW as including miscellaneous "satellite electronics from organizer on desk." These descriptions are not particularly helpful in identifying the property in dispute;

however, Harrell's motion treats items 020SW and 022SW as referring to property described in four of Clifford's analysis reports (Ex. S in support of Harrell's motion), and so, we do the same. We also refer to these items as Clifford did in his analysis reports.

In the first of these reports, Clifford concluded that switches included in item 24G "are used in any multi-antenna requirement, legitimate or illegitimate," that item 24I is a general computer component and that "nothing makes [it] noteworthy regarding satellite television piracy," and that items 26P and 26Q "appear to have no piracy application." The government offered no evidence to contradict these conclusions; therefore, items 24G, 24I, 26P and 26Q are not contraband per se under section 1029(a)(9). Because the government agrees to return nine assorted computer cables and adaptors included in item 24E, this item is not in dispute.

[9] In the second report, Clifford concluded that "[t]here are no known legitimate purposes for the possession of [items 24C, 26C, 26F and 26G] other than to be used with satellite receivers for the reason of stealing satellite signals." All of these items are "locks," used in the pirate community to interrupt signal commands sent to receivers. Clifford explained that these "locks" allow the user to "control whether [receivers] accept certain updates in order to keep [them] from accepting Electronic Countermeasures sent by Dish Network." Toy further explained that these locks "have no other purpose than stealing satellite signals as they are installed in the receiver so that the user can evade Electronic Countermeasures sent by DISH Network." While it is undisputed that Harrell possessed this hardware, the government failed to specifically show that these "locks" are "configured to insert or modify telecommunication identifying information" pursuant to section 1029(a)(9). Clifford and Toy explained that these "locks" control receivers and keep them from accepting Electronic Countermeasures sent by the service provider DISH Network. However, that conclusion does not explain how, or

whether, "locks" in fact insert or modify "telecommunication identifying information" (i.e., boxkey identification numbers). Whether this is in fact the case requires a technical electronic analysis that is not in the record. Therefore, the government failed to meet its burden of showing these "locks" to be contraband per se. We do not decide whether these "locks" could be contraband per se under another statutory provision, as that issue is not before us; nor do we foreclose the possibility that Congress may broaden section 1029(a)(9)'s language to account for technological developments in satellite television piracy in the future. However, here, because the government seeks to retain these "locks" pursuant to section 1029(a)(9), it bears the burden of showing that they "insert or modify telecommunication identifying information," and the government did not meet that burden.

[10] Clifford further noted in his second report that items 24F (satellite finder) and 26A (memory eraser), while they are used to pirate satellite television, have a commercial use. Toy also conceded that satellite finders and memory erasers have a commercial use. Therefore, these items are not contraband per se. Finally, Clifford concluded that items "24H, 24J-1, 24J-2, 26H and 26I are piracy devices." Items 24H, 26H and 26I are J-TAG interface devices and items 24J-1 and 24J-2 are Sombreros. Toy explained, that "J-TAG interface devices designed to function with DISH Network equipment have no other purpose than stealing satellite signals as they are piracy devices that aid in transferring piracy software between receivers and PC computers." Toy further explained that "Sombreros have no other purpose than stealing satellite signals as they are used to extract boxkeys from the memory of a DISH Network receiver." We conclude that items 24H, 26H, 26I, 24J-1 and 24J-2 are contraband per se under section 1029(a)(9) because they are configured to "insert or modify telecommunication identifying information."

[11] In the third report, Clifford found items 24B, 24D, 26B, 26J, 26L and 26N to be "potentially associated with the

piracy of DirecTV materials," and stated that they had to be submitted for "proper identification" and "forensic analysis." Items 24B and 26B are card programmers, items 24D, 26J and 26L are described as Shadow II and Chamelon piracy devices, and item 26N is an ISO bootloader. There is no record evidence that any of these items were ever analyzed, nor is there any record evidence indicating the results of this analysis, if it did in fact take place. The only additional record evidence pertaining to these items is Toy's explanation that smartcard programmers have a legitimate commercial business use. Therefore, the government did not meet its burden of showing these items to be contraband per se under section 1029(a)(9).

Clifford's fourth report includes another Sombrero, item 24A, which Toy stated has "no other purpose than stealing satellite signals." Again, because this item is configured to "insert or modify telecommunication identifying information," it is contraband per se under section 1029(a)(9). As for the remaining five items in this report, 26D, 26E, 26K, 26M and 26O, Clifford's report indicates that these items are configured to insert or modify telecommunication identifying information, and Toy explained that they "serve no other purpose than to pirate satellite signals." Specifically, item 26D consists of ATMEGA 128 piracy devices, which are used in lieu of smartcards and are "programmed to receive a pirated satellite signal," item 26E consists of DSSREV piracy devices, which are also used in lieu of smartcards, and items 26K, 26M and 26O consist of audio video replicators and their respective programmers, which are used to transfer piracy software and program piracy devices. As each of these items are configured to "insert or modify telecommunication identifying information," they are contraband per se under section 1029(a)(9).

Finally, the Department Evidence Report describes item 021SW as miscellaneous compact discs with satellite programs. The property encompassed in item 021SW appears to correlate with the property in one of Clifford's reports (Ex. T

in support of Harrell's motion). Of the six items included in this report, Harrell seeks the return of only two, items 25A and 25B5. Clifford concluded that item 25A contains "software for a 3D/4D Brower [sic] Mouse." As there is no record evidence that this item is contraband per se, it must be returned to Harrell. Harrell argues that item 25B5 must also be returned to him because it is a compact disc that "contains music downloads and internet shortcuts that have nothing to do with alleged satellite signal piracy." However, Clifford's report indicates that in addition to these downloads and shortcuts, item 25B5 also contains "satellite television piracy material regarding the extraction of DISH Network boxkeys from various receivers through their respective JTAG terminal." Toy also concluded that "instructions on the extraction of boxkeys . . . serve no purpose other than to pirate satellite signals." As Harrell "does not seek the return of any discs containing downloaded instructions explaining how to modify equipment to permit the illegal viewing of encrypted television signals," item 25B5 need not be returned to Harrell.

The government agrees to return the remaining seized property to Harrell. This property includes two hard drives (002CS, 003CS), a remote control (010SW), a computer (034SW), and four unmodified DISH Network blue cards included in item 032SW (416986, 821637, 069703, 673556). Harrell does not seek the return of a fifth modified blue card (803651). The government has already returned shipping paperwork, envelopes, and miscellaneous paperwork (018SW) and one computer (033SW) to Harrell.

IV. Conclusion

On remand, the government must return the following items to Harrell: 001SW, 002SW, 003SW, 004SW, 005SW, 006SW, 007SW, 008SW, 009SW, 011SW, 012SW, 013SW, 014SW, 015SW, 016SW, 017SW, 019SW, 023SW, 024SW, 025SW, 026SW, 027SW, 028SW, 029SW, 030SW, 031SW, 24E, 24G, 24I, 26P, 26Q, 24C, 26C, 26F, 26G, 24F, 26A,

24B, 24D, 26B, 26J, 26L, 26N, 25A, 002CS, 003CS, 010SW, 034SW, and four of item 032SW's DISH Network blue cards (416986, 821637, 069703, 673556). The government has already returned items 018SW and 033SW to Harrell, and the government may retain the remaining property.

AFFIRMED IN PART, REVERSED IN PART, and REMANDED for proceedings consistent with this opinion. Each party shall bear its own costs on appeal.