

**UNITED STATES DISTRICT COURT  
MIDDLE DISTRICT OF FLORIDA  
TAMPA DIVISION**

**DISH NETWORK L.L.C., ECHOSTAR  
TECHNOLOGIES L.L.C. AND  
NAGRASTAR L.L.C.,**

**Plaintiffs,**

**v.**

**Case No. 8:08-cv-590-T-30TBM**

**ROBERT WARD,**

**Defendant.**

\_\_\_\_\_ /

**ORDER**

THIS CAUSE comes before the Court upon Plaintiffs' Motion for Summary Judgment (Dkt. 59), Defendant's Response and Memorandum in Opposition to same (Dkts. 66-67), and Plaintiffs' Reply (Dkt. 75). The Court, having reviewed the motion, response, reply, record evidence, and being otherwise advised in the premises, concludes that Plaintiffs' Motion for Summary Judgment should be granted.

**BACKGROUND**

**I. Plaintiffs' Subscription-Based Satellite Television Programming**

Plaintiffs DISH Network L.L.C., EchoStar Technologies L.L.C., and NagraStar L.L.C. (collectively, "DISH Network") move for summary judgment against Defendant Robert Ward ("Ward") on Counts I and III of their Amended Complaint alleging violations of the Digital Millennium Copyright Act ("DMCA") and Communications Act.

DISH Network is a multi-channel video provider that delivers video, audio, and data services via a direct broadcast satellite system to more than 13 million subscribers throughout the United States. DISH Network uses high-powered satellites to broadcast, among other things, movies, sports, and general entertainment services (“DISH Network programming”) to consumers who have been authorized to receive such services after payment of a subscription fee, or in the case of a pay-per-view movie or event, the purchase price. DISH Network contracts for and purchases the distribution rights for most of the programming broadcast on the DISH Network platform from providers such as network affiliates, pay and specialty broadcasters, cable networks, motion picture distributors, sports leagues, event promoters, and other holders of programming rights.

DISH Network programming is digitized, compressed, and scrambled prior to being transmitted to multiple satellites. A DISH Network satellite television system consists of a compatible dish antenna, receiver, smart card which in some instances is internalized in the receiver, television, and cabling to connect the components. EchoStar Technologies designs and distributes receivers, dish antenna, and other digital equipment for the DISH Network satellite television system.

NagraStar provides smart cards and other technology to DISH Network that are part of a proprietary conditional access system known as Digital Nagra Advanced Security Process. DISH Network, in turn, provides the smart cards to its authorized subscribers. The NagraStar conditional access security system performs two interrelated functions in the ordinary course of its operation: (1) subscriber rights management, which allows DISH

Network to “turn on” and “turn off” programming a customer ordered, cancelled, or changed; and (2) protection of the global keys that are meant to descramble the DISH Network satellite signal, which prevents unauthorized reception and viewing of DISH Network programming.

NagraStar’s conditional access system includes a smart card containing a secure embedded microprocessor that functions as a security computer. The microprocessor has a ROM segment of memory that provides instructions and commands to the smart card in the everyday operation of the NagraStar security system. The ROM segment reads from data stored in the microprocessor’s EEPROM memory segment in order to perform its calculation and operation functions. The EEPROM memory segment also stores a special kind of data, called “decryption keys,” which are used to protect global video decryption keys.

After software in the smart card determines that a subscriber is tuned to a channel he is authorized to watch, the smart card transmits the current decryption key to the EchoStar Technologies receiver to decrypt the DISH Network signal. The decryption key changes periodically and DISH Network may broadcast messages announcing these changes weekly, daily, or even hourly. The EchoStar Technologies receiver forwards each new decryption key to the smart card, which stores the key in its EEPROM for later use. Together, the receiver and smart card convert DISH Network’s scrambled satellite signal broadcasts into viewable programming that can be displayed on the attached television of a DISH Network subscriber.

## **II. Piracy of DISH Network Programming Using Free-To-Air Receivers**

Pirates recently developed a means to circumvent the DISH Network security system and intercept DISH Network satellite broadcasts using free-to-air (“FTA”) receivers. FTA receivers were originally used in receiving unencrypted, freely available satellite transmissions. FTA broadcasts tend to be limited to ethnic, religious, and advertising content, and do not carry the more sought-after programming channels found in subscription television packages such as DISH Network.

Pirating DISH Network programming with an FTA receiver is accomplished by loading software that contains the proprietary software and keys to DISH Network’s security system (hereinafter, “piracy software”) onto the circuit chips on the FTA receiver, so as to mimic a DISH Network access card. Piracy software is made freely available on internet websites and, once downloaded, transferred to an FTA receiver through a connection to a home computer or thumb drive. The process of loading piracy software is referred to as “flashing” the FTA receiver and can be completed in minutes.

DISH Network, EchoStar Technologies, and NagraStar suffer harm from FTA receiver piracy, including lost subscription revenues that average about \$70 per month for an authorized customer. Pirates with modified FTA receivers have unlimited access to DISH Network programming, including premium and pay-per-view channels, the value of which exceeds that built into the average subscriber calculation.

### **III. Record Evidence of Ward's Distribution of Piracy Software Using the Monikers "Thedssguy and Veracity"**

The record reflects that Ward, using the monikers "Thedssguy" and "Veracity" posted files that would allow unauthorized receivers to circumvent the DISH Network security system. Specifically, the record reflects evidence that Ward was known as "Thedssguy" and "Veracity" in the free-to-air piracy community and that Thedssguy and Veracity made multiple forum posts that can be traced back to Ward. For example, through these monikers, the record reflects that Ward referred to himself by name, and provided his own date of birth, telephone number, street addresses, and email address. The declarations and attached documents show that there were multiple postings that provided details about this lawsuit, discussed specifics about Ward's criminal record, and revealed facts about Ward's family members and personal acquaintances. Plaintiffs also rely upon declarations and communications seized from computers during piracy raids, to demonstrate that Ward used these monikers.

The record also reflects that the monikers "Thedssguy" and "Veracity" posted approximately 47 software files that allowed a certain brand of FTA receiver to circumvent the DISH Network security system and intercept DISH Network programming, and had no other commercially significant purpose or use. The record shows that these 47 software files were downloaded multiple times.

### **IV. Ward's Pending Criminal Case and Invocation of the Fifth Amendment Privilege against Self-Incrimination**

Ward was indicted by a California federal grand jury on July 9, 2009, charging him with one count of conspiracy to violate the DMCA. Ward was arrested in Seminole, Florida on July 13, 2009 by the Federal Bureau of Investigation, and later released from custody on \$25,000 bond. Following removal, Ward pled not guilty at an arraignment before the United States District Court for the Southern District of California.

On August 6, 2009, Ward's deposition was taken. During his deposition, Ward refused to answer most of the questions on the basis that doing so would incriminate him. On October 26, 2009, Ward filed a Motion to Stay this case based on the pending criminal case (Dkts. 63-64). On November 9, 2009, Plaintiffs filed a Response in Opposition to Ward's Motion to Stay (Dkt. 70). Prior to the Court's ruling on Ward's Motion to Stay, the parties filed a Joint Motion for Limited Trial Continuance and Request to Moot Defendant's Pending Motion to Stay (Dkt. 71), which this Court subsequently granted (Dkt. 72).

The Joint Motion stated that on October 14, 2009, Ward entered into a plea agreement with the United States Attorneys' Office for the Southern District of California in which he pleaded guilty to conspiracy to hack DISH Network's Nagra3 security technology. The Joint Motion also indicated that Ward's sentencing was scheduled on January 29, 2010, and that the parties requested a stay of the trial in this case until after Ward's sentencing. The stay, however, was not to have any effect on the Court's determination of Plaintiffs' pending Motion for Summary Judgment.

## **DISCUSSION**

### **I. Summary Judgment Standard**

Motions for summary judgment should only be granted when the pleadings, depositions, answers to interrogatories, and admissions on file, together with the affidavits, show there is no genuine issue as to any material fact and that the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(c); Celotex Corp. v. Catrett, 477 U.S. 317, 322 (1986). The existence of some factual disputes between the litigants will not defeat an otherwise properly supported summary judgment motion; “the requirement is that there be no *genuine issue of material fact*.” Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 248 (1986) (emphasis in original). The substantive law applicable to the claimed causes of action will identify which facts are material. Id. Throughout this analysis, the court must examine the evidence in the light most favorable to the non-movant and draw all justifiable inferences in its favor. Id. at 255.

Once a party properly makes a summary judgment motion by demonstrating the absence of a genuine issue of material fact, whether or not accompanied by affidavits, the nonmoving party must go beyond the pleadings through the use of affidavits, depositions, answers to interrogatories and admissions on file, and designate specific facts showing that there is a genuine issue for trial. Celotex, 477 U.S. at 324. The evidence must be significantly probative to support the claims. Anderson, 477 U.S. at 248-49 (1986).

This Court may not decide a genuine factual dispute at the summary judgment stage. Fernandez v. Bankers Nat’l Life Ins. Co., 906 F.2d 559, 564 (11th Cir. 1990). “[I]f factual issues are present, the Court must deny the motion and proceed to trial.” Warrior Tombigbee Transp. Co. v. M/V Nan Fung, 695 F.2d 1294, 1296 (11th Cir. 1983). A dispute about a

material fact is genuine and summary judgment is inappropriate if the evidence is such that a reasonable jury could return a verdict for the nonmoving party. Anderson, 477 U.S. at 248; Hoffman v. Allied Corp., 912 F.2d 1379 (11th Cir. 1990). However, there must exist a conflict in substantial evidence to pose a jury question. Verbraeken v. Westinghouse Elec. Corp., 881 F.2d 1041, 1045 (11th Cir. 1989).

## **II. Ward's Invocation of the Fifth Amendment Privilege**

The Court initially considers the implications of Ward's assertion of Fifth Amendment privileges on the pending summary judgment motion. As set forth herein, Ward repeatedly invoked his Fifth Amendment right not to incriminate himself during his deposition. See U.S. Const. amend V.

It is well-established that litigants in civil cases may decline to testify if their testimony would tend to incriminate them in a criminal proceeding. See Wehling v. Columbia Broadcasting Sys., 608 F.2d 1084, 1086 (5th Cir. 1979), reh'g denied, 611 F.2d 1026 (5th Cir. 1980). The Supreme Court has held that a civil litigant who chooses to assert his Fifth Amendment privilege may not suffer "the imposition of any sanction which makes assertion of the Fifth Amendment privilege 'costly.'" Spevack v. Klein, 385 U.S. 511, 515 (1967). Courts repeatedly have held, however, that an adverse evidentiary inference may be drawn against a party who refuses to testify, and although that adverse inference alone is not sufficient to warrant summary judgment, summary judgment may be appropriate if supported by independent evidence. Baxter v. Palmigiano, 425 U.S. 308, 317-18 (1976); Avirgan v.

Hull, 932 F.2d 1572, 1580 (11th Cir. 1991); Fed. Trade Comm'n v. Global Mktg. Group, Inc., 594 F. Supp. 2d 1281, 1288-89 (M.D. Fla. 2008).

The Court is in that precise position here. Plaintiffs have supported their statement of material facts with an extensive factual record, including numerous declarations with attachments, discovery documents, and expert reports to show that Ward used the monikers “Thedssguy” and “Veracity” to post and distribute piracy software and information on the Internet in violation of the DMCA and the Communications Act. Ward has failed to refute any allegations of undisputed fact offered by Plaintiffs except to summarily state that Plaintiffs’ evidence shows that there is a genuine issue of fact concerning whether Ward actually sent or posted the piracy software on the Internet and in messages. Specifically, Ward argues that multiple people lived at his address and could have accessed his computer, i.e., his son, with whom he operated a business, could have sent the piracy software, and/or that a computer hacker could have sent the piracy software. Ward’s arguments, however, are nothing more than blanket denials, and are unsupported in the record.

Importantly, Rule 56 (e) requires the nonmoving party to proffer evidence to establish that a reasonable jury could rule in his favor: “The movant has the burden of showing that there is no genuine issue of fact, but the [nonmovant] is not thereby relieved of his own burden of producing in turn evidence that would support a jury verdict.” Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 255, 106 S.Ct. 2505, 2514, 91 L.Ed.2d 202 (1986). See also, Addickes v. S.H. Kress & Co., 398 U.S. 144, 90 S.Ct. 1598, 26 L.Ed.2d 142 (1970); First National Bank of Arizona v. Cities Service Co., 391 U.S. 253, 287, 88 S.Ct. 1575, 1592, 20

L.Ed.2d 569 (1968). The nonmovant may not rest solely on the allegations or denials in his pleading; he must present specific facts showing that there is a genuine issue of material fact for trial. Fed.R.Civ.P. 56(e); Anderson, 477 U.S. at 255, 106 S.Ct. at 2514; Young v. City of Palm Bay, 358 F.3d 859, 869 (11th Cir. 2004).

The Court has examined the factual record in detail and finds that Plaintiffs have submitted significant independent admissible evidence of Ward's violations of the DMCA and the Communications Act. The Court relies principally on this independent factual record, rather than on any adverse inference, to establish grounds for this grant of summary judgment.<sup>1</sup>

### **III. Legal Analysis**

#### **A. Count I - The Digital Millennium Copyright Act**

The DMCA, 17 U.S.C. §1201(a)(2), prohibits persons from providing or offering to the public any technology that satisfies one of three criteria: (1) the technology is designed or produced for circumventing a measure that controls access to a copyrighted work; (2) the

---

<sup>1</sup> Notably, although Ward pleaded guilty to conspiracy to hack DISH Network's Nagra3 security technology in the pending criminal action, the Court does not consider that evidence in granting summary judgment, because, as set forth in Plaintiffs' Opposition to Ward's Motion to Stay (Dkt. 70), the pending criminal action deals with conduct that "largely took place after the filing of this case" and "DISH Network is not asserting claims against Ward [in this case] based on his efforts to crack the new DISH Network smart card."

technology has only a limited commercial purpose or use other than for circumventing an access control measure; or (3) the technology is marketed for use in circumventing an access control measure. For purposes of the statute, circumventing an access control measure means to “descramble a scrambled work, to decrypt an encrypted work, or to otherwise avoid, bypass, remove, deactivate, or impair a technological measure.” 17 U.S.C. §1201(a)(3)(A).

DISH Network moves for summary judgment on Count I of the Amended Complaint alleging violations of the DMCA, arguing that there is irrefutable evidence that Ward, using the monikers “Thedssguy” and “Veracity,” engaged in the internet-based distribution of software that enabled FTA receivers to circumvent the DISH Network security system. The Court agrees. As set forth herein, the record reflects that DISH Network security system is an effective technological measure under the DMCA. The record also reflects that Ward used the monikers “Thedssguy” and “Veracity” to offer and provide on the internet a form of circumvention technology that violates the DMCA. Lastly, the record reflects that the software files enabled FTA receivers to circumvent the DISH Network security system, and had no other commercially significant purpose or use.

The Court also concludes, as set forth herein, that Ward has not rebutted Plaintiffs’ evidence and that Ward’s denials and suppositions regarding other people who could have posted the offending files, insufficient to create a genuine issue of material fact for trial. Accordingly, Plaintiffs’ Motion for Summary Judgment as to Count I of the Amended Complaint is granted.

**B. Count III - The Communications Act**

Plaintiffs argue that Ward's same behavior (as they allege under the DMCA) of distributing piracy software files for FTA receivers similarly violates the Communications Act, 47 U.S.C. §605(e)(4). Ward argues that 47 U.S.C. §605(e)(4) does not cover the distribution of piracy software.<sup>2</sup>

Section 605(e)(4) of the communications Act provides:

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. 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.

47 U.S.C. §605(e)(4) (emphasis added). Subsection (a) prohibits persons from receiving or assisting in receiving, without authorization, subscription-based satellite television programming such as DISH Network. 47 U.S.C. §605(a). Plaintiffs argue that Ward's piracy software is both a "device" and "equipment" prohibited by section 605(e)(4). Defendant disagrees. It appears that this is a matter of first impression.<sup>3</sup>

---

<sup>2</sup> The Court entered an order requesting that Plaintiffs brief this issue, because Plaintiffs' Motion for Summary Judgment did not cite any authority suggesting that Section 605(e)(4) covered the distribution of software and the Court did not locate any case law directly on this issue (Dkt. 74). Plaintiffs subsequently filed their reply on this issue (Dkt. 75).

<sup>3</sup> In DirecTV, Inc. V. Hughes, No. 5:03-cv-148, 2005 WL 3776347, \*2 (W.D. Mich. May 17, 2007), the court awarded statutory damages for violation of section §605(e)(4) based on the defendant's internet-based distribution of piracy software. However, the damages were awarded based on the defendant's default, because the defendant failed to appear or defend the action, and  
(continued...)

Plaintiffs argue in their reply that the ordinary meaning of the phrase “electronic, mechanical, or other device or equipment” encompasses Ward’s piracy software. Plaintiffs also point the Court to related statutes that support application of Section 605(e)(4) to piracy software. Plaintiffs also note that the United States Department of Justice has successfully prosecuted numerous satellite pirates involved in writing and distributing illicit software pursuant to section 605(e)(4) of the Communications Act.

The Court concludes that section 605(e)(4) covers piracy software. The Court agrees that the plain meaning of the terms “device” and “equipment” include software. See Dictionary.com Unabridged (Random House, Inc.), <http://dictionary.reference.com> (last visited Jan. 7, 2010) (defining “device” as “a thing made for a particular purpose; an invention or contrivance, esp. a mechanical or electrical one” and defining “equipment” as “anything kept, furnished, or provided for a specific purpose”). The Court also finds it significant that Section 153(45) of the Communications Act, which is applicable to all of Chapter 5 concerning wire and radio communications, which includes section 605(e)(4), defines “telecommunications equipment” to include “software integral to such equipment.” 47 U.S.C. §153(45).

---

<sup>3</sup>(...continued)  
the issue of whether §605(e)(4) applied to software was not brought to the court’s attention. Id.

Lastly, the Court is persuaded by Plaintiffs' identification of several state statutes<sup>4</sup> modeled after section 605(e)(4), which support a plain meaning of "device" that includes software and by the fact that the distribution of piracy software is prosecuted under section 605(e)(4).

As set forth herein, the record is undisputed that Ward distributed piracy software on internet websites. The record also reflects that Ward knew that the software was primarily of assistance in the unauthorized decryption of the DISH Network signal. Accordingly, Plaintiffs' Motion for Summary Judgment as to Count III of the Amended Complaint is granted.

### **C. Damages**

Plaintiffs seek statutory damages, injunctive relief, and attorneys' fees and costs. The law is clear that a plaintiff cannot recover duplicative statutory damages under different legal theories where the conduct underlying the claims is the same and DISH Network elects to recover under only one statute (Dkt. 75). The Court concludes that the facts of this case are more relevant to the DMCA and that it would be most appropriate to award damages under that statute. See Tu v. TAD System Technology Inc., 2009 WL 2905780, \*5 (E.D.N.Y. Sept. 10, 2009) (deciding that damages should be awarded under the Copyright Act, because it was the "most appropriate remedy").

---

<sup>4</sup> See Fla. Stat. §§812.15(1)(c), (2)(a); Pa. Cons. Stat. Ann. §§910(a)-(e); Del. Code Ann. Tit. 11, §§850(a)-(e); Md. Code Ann. §§7-313(c), 7-315, 7-318; Va. Code Ann. §§ 18.2-190.2-190.8.

In lieu of actual damages and profits, a prevailing plaintiff under the DMCA may elect to recover “statutory damages for each violation of 1201 in the sum of not less than \$200 or more than \$2,500 per act of circumvention, device, product, component, offer, or performance of service, as the court considers just.” 17 U.S.C. §1203(c)(3)(A). The DMCA makes clear that Plaintiffs are entitled to statutory damages for “each violation.” In Stockwire Research Group, Inc. v. Lebed, the court held that “each violation” was to be determined on a per download basis. 577 F. Supp. 2d 1262, 1268 (S.D. Fla. 2008).

The record reflects that Ward offered and provided 255,741 piracy software files to end-users. (SOUF 73-74). At the minimum statutory penalty of \$200 per download, statutory damages amount to \$51,148,200 (255,741 x \$200).

The DMCA and Communications Act authorize courts to grant permanent injunctions on reasonable terms. 17 U.S.C. §1203(b)(1); 47 U.S.C. §605(e)(3). The Court concludes that under the facts of this case, Plaintiffs are entitled to a permanent injunction. Plaintiffs have established that Ward’s distribution of piracy software caused substantial and unquantifiable harm in that he enabled an untold number of end-users to circumvent the DISH Network security system and intercept copyrighted DISH Network programming. A permanent injunction is also necessary to prevent Ward from engaging in future wrongful conduct because Plaintiffs do not have an adequate remedy to prevent damage they would suffer by further infringement by Ward.

Thus, Ward is permanently enjoined from creating or distributing any form of technology that is designed for, primarily used for, or marketed for circumventing the DISH

Network security system, or any technology otherwise of assistance in intercepting DISH Network programming. Ward should be further enjoined from engaging in any form of circumvention or interception with respect to DISH Network's security system or satellite signal, or assisting any other person in same.

The Communications Act provides that a court "shall direct the recovery of full costs, including awarding reasonable attorneys' fees to an aggrieved party who prevails" under section 605(e)(4). 47 U.S.C. §605(e)(3)(B)(iii). The DMCA also authorizes recovery of attorneys' fees and costs by a prevailing party. 17 U.S.C. §1203(b)(4)-(5).

The Court concludes that this case is appropriate for the award of reasonable attorneys' fees and costs. Plaintiffs are directed to submit to the Court, within thirty (30) days from the date of his Order, an affidavit specifying the attorneys' fees and costs incurred. The affidavit is required to be detailed and should describe the specific work performed by each timekeeper on each day, the time expended for the services performed each day, and the hourly rate charged by each attorney and staff member who performed services.

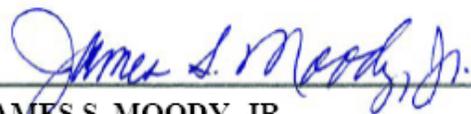
### **CONCLUSION**

For the reasons set forth herein, it is ORDERED AND ADJUDGED that:

1. Plaintiffs' Motion for Summary Judgment (Dkt. 59) is hereby GRANTED.
2. The CLERK is directed to enter Judgment in favor of Plaintiffs and against Defendant in the sum of \$51,148,200.

3. Defendant is PERMANENTLY ENJOINED from creating or distributing any form of technology that is designed for, primarily used for, or marketed for circumventing the DISH Network security system, or any technology otherwise of assistance in intercepting DISH Network programming. Defendant is PERMANENTLY ENJOINED from engaging in any form of circumvention or interception with respect to DISH Network's security system or satellite signal, or assisting any other person in same.
4. Plaintiffs are directed to submit to the Court, within thirty (30) days from the date of his Order, an affidavit specifying the attorneys' fees and costs incurred.

**DONE** and **ORDERED** in Tampa, Florida on January 8, 2010.

  
\_\_\_\_\_  
**JAMES S. MOODY, JR.**  
**UNITED STATES DISTRICT JUDGE**

**Copies furnished to:**

Counsel/Parties of Record  
S:\Even\2008\08-cv-590.frm