1

2   **E-Filed 3/9/2011**

3

4

5

6

7   **IN THE UNITED STATES DISTRICT COURT**

8   **FOR THE NORTHERN DISTRICT OF CALIFORNIA**

9   **SAN JOSE DIVISION**

10   DISH NETWORK, L.L.C., a Colorado Limited   Case Number 5:08-cv-01561 JF (PSG)
     Liability Company; ECHOSTAR
11   TECHNOLOGIES, L.L.C., a Texas Limited   **ORDER[1] GRANTING PLAINTIFFS'**
     Liability Company; NAGRASTAR, L.L.C., a   **MOTION FOR SUMMARY**
12   Colorado Limited Liability Company,   **JUDGMENT**

13   Plaintiffs,   [Re: Docket No. 44]

14   v.

15   SatFTA a.k.a. SERGIO ALEXEYEV,

16   Defendant.

17

18   Plaintiffs DISH Network L.L.C., Echostar Technologies, L.L.C., and Nagrastar, L.L.C.

19   (collectively, "Plaintiffs") seek summary judgment against Defendant SatFTA a.k.a. Sergio

20   Alexeyev ("Defendant") for alleged violations of the Digital Millennium Copyright Act, 17

21   U.S.C. §§ 1201(a)(1)-(2) and (b)(1) ("DMCA"); the Communications Act of 1934, as amended,

22   47 U.S.C. § 605(a); and the California Penal Code §§ 593(d) and (e). Having considered the

23   evidence presented by Defendant, the Court concludes that no reasonable jury could find in his

24   favor. Accordingly, summary judgment will be granted.

25   **I. BACKGROUND**

26   This action arises out of Defendant's creation and distribution of various program files

27

28   _____

          [1] This disposition is not designated for publication.

     Case Number 5:08-cv-01561 JF (PSG)
     ORDER GRANTING PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT
     (JFLC1)

capable of circumventing the DISH Network security system. DISH Network is a subscription-based satellite broadcast provider. Duval Decl. ¶ 4. EchoStar supplies all satellite dishes and receivers as well as all NagraStar access cards ("smartcards") to DISH Network subscribers. *Id.*

A. **Program Files**

Defendant admits to developing and posting several program files to the following piracy websites under the username SatFTA: (1) www.id-discussions.com; (2) www.dsschat.com; (3) www.innermatrix.net; (4) and www.sattech.net (collectively "the Piracy Websites"). Cmplt. ¶ 54; Response to Plaintiffs' First Set of Requests for Admission, Nos. 1-4, 6-8, 54-57, 69-72, 76-79, 81-84, 93-96, 100-103, 108-111 ("RFA Resp.").[2]

IRDr.exe

The IRDR.exe program facilitates the unauthorized re-programming of DISH Network smartcards by extracting box-keys from DISH Network receivers. RFA Resp. No. 62; Haugsness Decl. ¶ 14. Each receiver contains unique box-keys, and smartcards work with a receiver only when they are programmed with that receiver's keys. Haugsness Decl. ¶ 12; Alexeyev Depo. 65:1-8. Once the IRDR program reads the box-keys, the box-keys can be programmed onto a smartcard, allowing non-subscribers to gain access to DISH Network programming. Haugsness Decl. ¶ 14. Defendant posted at least 100 iterations of this program on the aforementioned websites, and the program was downloaded 5,809 times. Alexeyev Depo. 126:8-16; Haugsness Decl. ¶ 16.

IRDcM.exe

IRDcM.exe extracts DISH Network channel listing tables from DISH Network satellite receivers. Haugsness Decl. ¶¶ 18-19. Channel listing tables typically are used in piracy programs to assign authorizations in a smartcard, which would allow individuals to receive DISH Network programming without a subscription. *Id.*; Alexeyev Depo. 132:9-19. Defendant posted the IRDcM program on the Piracy Websites, and posted five channel tables generated

---

[2] Defendant does not dispute that the websites contained information relating to satellite piracy, but he argues that they also offer a host of products, hardware, and forums related to a variety of topics. RFA Resp. Nos. 58-61; Opp. Br. at 15

2

from that program on the Id-discussions and Innermatrix sites.[3] RFA Resp. Nos. 76-79;

Alexeyev Depo. 221:19-226:3.

PVRdSE.exe

The PVRdSE.exe program allows users to copy the programming content recorded on the

hard-drive of a DISH Network PVR satellite receiver to a computer hard-drive.[4] RFA Resp. No.

80. After a DISH Network PVR hard-drive is removed from the receiver and installed into a

personal computer ("PC"), the PVRdSE program overcomes DISH Network's copy-control

measure to allow the computer to recognize the PVR hard-drive and load the recordings

contained therein. Haugsness Decl. ¶ 22. Once a copy of the recordings have been saved onto a

PC, individuals are free to make and distribute unauthorized copies of the recordings. *Id.* ¶ 23.

Defendant posted the PVRdSE program on the Piracy Websites, and it was downloaded at least

1,525 times. *Id.* ¶ 24; RFA Resp. Nos. 81-84.

i2c.jpg

i2c.jpg is a diagram that can be used to build a connector to interface with the electrically

erasable programmable read only memory ("EEPROM") in a DISH Network receiver. RFA

Resp. No. 91. In DISH receivers, the EEPROM stores information relating to electronic

countermeasures ("ECMs") that are used to disable piracy devices. Haugsness Decl. ¶ 27.

Using the 12c.jpg diagram, individuals can erase the data caused by DISH Network's ECMs and

continue receiving unauthorized programming. *Id.* Defendant posted this diagram to the Piracy

Websites. RFA Resp. Nos. 93-97.

jtag-pcb2.bmp

The jtag-pcb2.bmp diagram allows users to recover from ECMs. RFA Resp. No. 106. It

details the circuit layout required to interface with the software of DISH Network satellite

---

[3] Collectively, the tables were downloaded a total of 3,894 times. Exs. 19-24 to
Haugsness Decl.

[4] PVR receivers allow customers to record DISH Network programming. Haugsness
Decl. ¶ 21. Programming is saved in a format that cannot be read by non-DISH Network
computer systems. *Id.*

3

receivers. *Id.* No. 104. The diagram was posted by Defendant on the Piracy Websites. *Id.* Nos. 108-111.

jm.gif

jm.gif is a diagram that demonstrates how to program a pirate device to work with DISH Network receivers. *Id.* No. 99. By identifying the memory address of the box-keys in the receivers, it reveals the location of data that secures communication between receivers and smartcards. *Id.* No 97; Haugsness Decl. ¶ 25. Defendant posted this diagram on the Piracy Websites. RFA Resp. Nos. 100-103.

B. Seizure of Defendant's Piracy Devices

In March 2006, the FBI seized approximately twenty DISH Network receivers, fifteen DISH Network smartcards, and several smartcard re-programmers from Defendant's residence. Alexeyev Depo. 175:19-176:1, 72:19-73:5, 76:3-7, 177:11-17, 180:19-181:6. Defendant was not a DISH Network subscriber during the time he possessed this equipment.[5] Alexeyev Depo. 251:12-252:8. DISH Network engineers discovered that thirteen of the receivers contained signs of modification and four showed signs of ECM attacks. DeLyser Decl. ¶¶ 8-9, 12, Exs. 1-5 to DeLyser Decl. Additionally, Plaintiffs' piracy analysis revealed that five smartcards had been modified for unauthorized receipt of DISH Network programming. McMullen Decl. ¶¶ 5-16, Exs. 1-5 to McMullen Decl.

II. LEGAL STANDARD

A motion for summary judgment should be granted if there is no genuine issue of material fact and the moving party is entitled to judgment as a matter of law. Fed. R. Civ. P. 56(c); *Anderson v. Liberty Lobby, Inc.,* 477 U.S. 242, 247-48, 106 S.Ct. 2505, 91 L.Ed.2d 202 (1986). The moving party bears the initial burden of informing the Court of the basis for the motion and identifying the portions of the pleadings, depositions, answers to interrogatories, admissions, or affidavits that demonstrate the absence of a triable issue of material fact. *Celotex Corp. v. Catrett,* 477 U.S. 317, 323, 106 S.Ct. 2548, 91 L.Ed.2d 265 (1986).

---

[5] Defendant did not obtain a DISH Network subscription until 2008. Alexeyev Depo. 251:12-252:8.

4

If the moving party meets this initial burden, the burden shifts to the non-moving party to present specific facts showing that there is a genuine issue for trial. Fed. R. Civ. P. 56(e); *Celotex,* 477 U.S. at 324. A genuine issue for trial exists if the non-moving party presents evidence from which a reasonable jury, viewing the evidence in the light most favorable to that party, could resolve the material issue in his or her favor. *Anderson,* 477 U.S. 242, 248-49, 106 S.Ct. 2505, 91 L.Ed.2d 202; *Barlow v. Ground,* 943 F.2d 1132, 1134-36 (9th Cir. 1991). However, "[a] non-movant's bald assertions or a mere scintilla of evidence in his favor are both insufficient to withstand summary judgment." *F.T.C. v. Stefanchik*, 559 F.3d 924, 929 (9th Cir. 2009).

III. DISCUSSION

A. Counts I-II: Violations of the DMCA

Plaintiffs allege that Defendant personally committed acts of piracy and assisted others in committing such acts in violation of the DMCA and Communications Act. Cmplt. ¶¶ 44-76.

1. DMCA Violations

Defendant has admitted to creating and distributing the IRDr, IRDcM, and PVRdSE software. RFA Resp. Nos. 2-4, 69-72, 76-79, 81-84. In addition, Defendant has admitted to creating and distributing the i2c.jpg, jm.gif, and jtag-pcb2.bmp diagrams. *Id.* Nos. 6-8, 93-96, 100-103, 108-111. Defendant also has admitted to modifying DISH Network smartcards[6] and receiving DISH Network programming without a subscription.[7]

Section 1201(a)(1) of the DMCA prohibits, in relevant part, the circumvention of, "a technological measure that effectively controls access to a work protected [by copyright.]" 17

---

[6] At Defendant's deposition, Plaintiffs' counsel asked Defendant how often he had used the NagraEdit software to modify DISH Network smartcards. Alexeyev Depo. 71:5-9. Defendant indicated that, "[i]t was necessary to do that often because [he had] limited number of receiver [*sic*], so [he] did probably [*sic*] few times in limited number of cards . . ." *Id.*

[7] Defendant also was asked if he was "using [Tsreader software] to get DISH Network channels without paying for it." Alexeyev Depo. 310:10-23. Defendant admitted receiving the unauthorized channels, but he indicated that he was "not using [the software] to watch. . . . [but] to check how [the software was] working." *Id.*

5

U.S.C. § 1201(a)(1). Section 1201(a)(2) of the DMCA prohibits:

> offer[ing] to the public, provid[ing], or otherwise traffic[king] in any technology, product, service, device, component, or part thereof, that--
>
>> (A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected [by copyright];
>>
>> (B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected [by copyright]; or
>>
>> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected [by copyright].

17 U.S.C. § 1201(a)(2).

Section 1201(b)(1) of the DMCA prohibits:

> offer[ing] to the public, provid[ing], or otherwise traffic[king] in any technology, product, service, device, component, or part thereof, that--
>
>> (A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner . . . in a work or a portion thereof;
>>
>> (B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner . . . in a work or a portion thereof; or
>>
>> (C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner . . . in a work or a portion thereof.

17 U.S.C. § 1201(b)(1)

a.   § 1201(a)(1) Violations

As a result of his admitted modification of DISH Network smartcards, Defendant is liable for personal violations of § 1201(a)(1) of the DMCA. Smartcards work to descramble DISH Network's satellite signals to allow viewing of copyrighted programming. Duval Decl. ¶ 8. Defendant's modification of the smartcards allowed him to bypass DISH Network's security measures and intercept its satellite programming. McMullen Decl. ¶ 5. Section 1201(a)(1) specifically proscribes the circumvention of such technology. Defendant contends that he

6

modified the smartcards only for the purpose of testing the operation of various receivers, not to receive an unauthorized satellite signal. Opp. Br. at 18-19. However, potential "lawful . . . use of circumvention devices does not relieve [the Defendant] from liability . . . under the DMCA." *Sony Computer Entm't Am., Inc. v. Divineo, Inc.*, 457 F. Supp. 2d 957, 965 (N.D. Cal. 2006)

Defendant also is liable under § 1201(a)(1) for modifications to DISH Network devices. DISH Network security engineers determined that five of the smartcards seized from Defendant's residence by the FBI had been modified for illegal receipt of DISH Network programming. McMullen Decl. ¶¶ 5-16, Exs. 1-5 to McMullen Decl. They determined that at least four of the seized receivers similarly were modified because the receivers had been hit by an ECM, whose only purpose is to target pirate activity. DeLyser Decl. ¶ 9. On the one hand, Defendant argues that the receivers contained ECM marks when he first obtained them. Alexeyev Decl. ¶ 4. On the other hand, he argues that the ECM marks could have been "induced by the Plaintiff or the FBI during its investigation." *Id.* Not only are these assertions contradictory, but Defendant offers no facts to support them.

b. § 1201(a)(2) Violations

Additionally, Defendant's development and distribution of the IRDr and IRDcM software along with that of the i2c.jpg, jtag-pcb2.bmp, and jm.gif diagrams violates § 1201(a)(2) of the DMCA. The primary purpose of both the software and diagrams is to circumvent security measures and facilitate the receipt of unauthorized satellite channels. Plaintiffs have presented sworn testimony from security engineer Kyle Haugsness explaining that the software files and diagrams were "primarily designed to facilitate DISH Network piracy." Haugsness Decl. ¶ 10. For example, the IRDr software is designed to circumvent DISH Network's conditional access system.[8] Similarly, the i2c and jtag diagrams provide instructions on how to modify the software contained in DISH Network receivers, which allows interception of DISH Network's encrypted satellite signals.

---

[8] This system serves as a security measure to protect copyrighted works and typically requires application of a decryption process with an authorized DISH Network smartcard to gain access to programming. MSJ at 12 n.2.

7

In direct contradiction to his previous admissions, Defendant asserts in his opposition papers that he did not create the i2c and jtag diagrams.[9] Even if this were true, he fails to rebut the evidence that his online postings of the diagrams and software files assisted others in unauthorized access of DISH Network programming. In fact, he admits in his declaration that "part of the passport's information [extracted by the IRDr program] could be used to steal DISH Network programming" and the channel tables generated by the IRDcM program "could be theoretically used for pirating." Alexeyev Decl. ¶¶ 5, 13. With respect to the diagrams, Defendant simply does not address whether his postings offered piracy technology to the public.

c. § 1201(b)(1) Violations

Finally, Defendant is liable for § 1201(b)(1) violations because of his development and distribution of the PVRdSE program. He admits that this program allows users to copy the programming of a DISH Network PVR satellite receiver to a computer hard-drive. RFA Resp. No. 80. DISH Network protects against unauthorized copying and distribution of recorded programming by saving the copyrighted programs in an unrecognizable format. Haugsness Decl. ¶ 21. Defendant contends that his program serves a legitimate function in that it allows individuals to create back-up copies of their DISH Network PVR recordings. Opp. Br. at 16. The Court considered a similar argument in *Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F.Supp.2d 913 (N.D.Cal. 2009), and determined that, "while the DMCA provides for a limited 'fair use' exception for certain end users of copyrighted works, the exception does not apply to manufacturers or traffickers of the devices prohibited by 17 U.S.C. § 1201(a)(2)." *Id.* at 942. Because Defendant's PVRdSE program acts by allowing a computer to overcome DISH Network's copy-control measures,[10] it falls within the definition of a prohibited device under § 1201(a)(2).

---

[9] "The JTAG diagram was created by TOMAS VLAD." Alexeyev Decl. ¶ 28. "I2C is an industrial standard bus . . . which I reposted from an Italian website . . . The developer's name was Claudio Lanconelli." *Id.* ¶ 31.

[10] Haugsness Decl. ¶ 22.

8

B. Count III: Communications Act Violations

The Communications Act prohibits receiving or assisting others in the unauthorized receipt of "any interstate or foreign communication by radio." 47 U.S.C. § 605(a). This Court has held that § 605(a) applies to the unlawful interception of satellite transmissions. *DirecTV v. Hendrix*, No. 04-0370, 2005 WL 757562, at *3 (N.D. Cal. Apr. 1, 2005).

As discussed above, the IRDr and IRDcM programs assist non-subscribers in accessing DISH Network programming. Additionally, the jm.gif file serves to facilitate piracy by identifying the memory address of the box keys of DISH Network satellite receivers. RFA Resp. No. 97. Defendant admits that this form of identification is required to program a pirate device to work with a DISH Network receiver. RFA Resp. No. 99. His posting of the IRDr, IRDcM, and jm.gif files falls within the conduct proscribed by § 605(a) because it assisted others in the unauthorized receipt of satellite transmissions.

Defendant argues that he is not subject to liability under the Communications Act because the primary purpose of the files was diagnostic. Opp. Br. at 13. However, § 605(a) liability is not dependent upon the intent of the individual assisting in theft. The fact that a file may have both legal and illegal uses does not preclude a finding that the defendant acted to assist in the unauthorized interception of programming. *See Continental Cablevision, Inc. v. Poll*, 124 F.3d 1044, 1048 (9th Cir. 1997).

Defendant also is liable for § 605(a) violations as a result of the modifications he made to DISH Network smartcards and receivers as described above. "[D]irect evidence of signal piracy is not required to prove unlawful interception." *DirecTV, Inc. v. Webb*, 545 F. 3d 837, 844 (9th Cir. 2008). In *Webb*, the Ninth Circuit upheld a grant of summary judgment based on defendant's possession of multiple modified smartcards and receivers that had not been activated with DirecTV and evidence that his system had been targeted by a DirecTV electronic countermeasure. *Id.* at 844-45. Here, Defendant has admitted to modifying several DISH Network smartcards and he possessed multiple receivers with signs of ECM damage. This is sufficient to permit an inference of a § 605(a) violation.

9

C. Counts IV-VI: Violations of California Penal Code § 593

Plaintiffs allege that Defendant has violated Cal. Penal Code § 593 by modifying DISH Network smartcards and receivers and assisting others in such modifications. Cmplt ¶¶ 44-57, 77-97. Specifically, they claim that Defendant's modification of DISH Network receivers violated § 593d(a)(1), which prohibits the making or maintaining of "an unauthorized connection . . . to any cable, wire, or other component of a multichannel video or information services provider's system or to a cable, wire or other media, or receiver that is attached to . . [the] provider's system."

Defendant's modification of DISH Network smartcards also allegedly violated § 593d(a)(4), which prohibits the making or maintaining of "any modifications or alterations to an access device that authorizes services." According to Plaintiffs, Defendant's development and distribution of the IRDR and IRDcM programs also demonstrates liability under § 593e(a) because the software files assist others in reprogramming unauthorized smartcards in violation of § 593e(a)'s proscription against the "modification or alteration [of] any device installed with the authorization of a subscription television system, for the purpose of intercepting, receiving, or using any program or other service carried by the subscription television system which the person is not authorized . . . to receive or use."

Finally, Plaintiffs claim that Defendant's development and distribution of the i2c and jtag diagrams violated § 593e(b) because these diagrams assisted in the unauthorized interception of satellite transmissions, and § 593e(b) makes it unlawful to distribute "or otherwise provide any device, any plan, or any kit for a device or for a printed circuit, designed in whole or in part to decode, descramble, intercept, . . . any encoded, scrambled, or other nonstandard signal carried by [a] subscription television system."

Defendant argues that liability is in dispute because, "[p]urpose is critical in deciding whether Defendant violated California Penal Code section 593 . . ." Opp. Br. at 14. He maintains that his purpose in modifying the DISH Network technology and creating/posting the above-mentioned files was diagnostic. *Id.* Because of this factual dispute, he asserts that it would be improper for the Court to grant summary judgment in favor of Plaintiffs. *Id.*

10

However, contrary to Defendant's assertions, § 593 requires only general intent, not a specific intent to aid in piracy. Sections 593d(a)(1), (d)(a)(4) and §§ 593e(a)-(b) specifically prohibit knowing and willful action. "As a general rule a statute proscribing willful behavior is a general intent offense." *People v. Johnson*, 67 Cal.4th 67, 72 (1998). In *People v. Prevost*, 60 Cal.4th 1382, 1392 (1998) the California Court of Appeals held that § 593d does not require specific intent to aid in the theft of cable television signals. The same is true with respect to § 593e. Defendant does not dispute that he knowingly and willfully modified DISH Network technology or assisted others in such modifications. Accordingly, there is no material factual dispute as to his § 593 liability.

D. <u>Damages, Attorneys' Fees, and Injunctive Relief</u>

Plaintiffs seek statutory damages in the amount of $1,000 per violation of § 1201 of the DMCA. The DMCA provides that "a complaining party may elect to recover an award of statutory damages for each violation of section 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 court in its discretion may reduce or remit the total award of damages in any case in which the violator sustains the burden of proving, and the court finds, that the violator was not aware and had no reason to believe that its acts constituted a violation." 17 U.S.C. § 1203(c)(5)(A); *See Craigslist, Inc. v. Mesiab*, No. C 08-05064 CW, 2010 WL 5300883, at *10 (N.D. Cal. Nov. 15, 2010).

Plaintiffs claim that an award of $1,000 per violation is reasonable given the fact that this sum represents minimum statutory damages under the Communications Act, and Plaintiffs have chosen only to seek damages under the DMCA. *See* 47 U.S.C. § 605(e)(3). However, because there is at least some evidence in the record that Defendant did not intend to facilitate piracy, the Court will exercise its discretion to award damages in the amount of $200 per violation of the DMCA.

There is precedent suggesting that violations of the DMCA should be construed on a per-download basis. *See DISH Network v. Ward*, No. 8:08-cv-00590-JSM, Dkt. 77 (M.D. Fla. Jan. 8, 2010); *Stockwire Research Group, Inc. v. Lebed*, 577 F. Supp. 2d 1262, 1268 (S.D. Fla. 2008).

Case Number 5:08-cv-01561 JF (PSG)
ORDER GRANTING PLAINTIFFS' MOTION FOR SUMMARY JUDGMENT
(JFLC1)

Courts also have reasoned that the DMCA damages provisions should be interpreted to allow statutory damages for each unlawful distribution or posting made by a defendant. *Stockwire*, 577 F. Supp. 2d at 1267; *McClatchey v. Associated Press*, No. 3:05-cv-145, 2007 WL 1630261, at *6 (W.D.Pa. June 8, 2007). Based on this calculation method, Plaintiffs request that damages be assessed as follows:

- IRDr: 5,809 end-user downloads x $200 = $1,161,800

- IRDcM: 4 postings by Defendant x $200 = $800

- Channel Tables: 3,894 end-user downloads x $200 = $778,800

- PVRdSE: 1,525 end-user downloads x $200 = $305,000

- i2c.jpg: 4 postings by Defendant x $200 = $800

- jm.gif: 4 postings by Defendant x $200 = $800

- jtag-pcb2.bmp: 4 postings by Defendant x $200 = $800

- 9 instances of Defendant's personal circumvention x $200 = $1,800

This would result in a total damage award of $2,250,600.

In addition to statutory damages, Plaintiffs request attorneys' fees and costs for all DMCA and Communications Act violations. An award of attorneys' fees is mandatory under the Communications Act. 47 U.S.C. § 605(e)(3)(B) ("The Court . . . shall direct the recovery of full costs, including awarding reasonable attorneys' fees to an aggrieved party who prevails."). The DMCA, however, leaves such an award to the Court's discretion. 17 U.S.C. § 1203(b)(4)-(5). Where, as here, willful violations of the DMCA are present, courts have found that an award of costs and attorneys' fees is appropriate. *Comcast of Ill. X, LLC v. Jung Kwak*, No. 03-00962 DAE, 2010 WL 3781768, at *2 (D. Nev. Sep. 17, 2010); *Sony Computer Entertainment America, Inc. v. Divineo, Inc.*, 457 F.Supp.2d 957, 967 (N.D.Cal. 2006). Accordingly, the Court will award attorneys' fees and costs for Defendant's violations of the DMCA and Communications Act in an amount to be determined. Counsel for Plaintiffs will be directed to submit an itemized declaration.

Finally, Plaintiffs urge the Court to enjoin Defendant permanently from creating or distributing technology that is designed, used, or marketed for circumvention of the DISH

12

Network security system, or any technology that is capable of assisting in the interception of DISH Network programming. They also request that the Court enjoin Defendant permanently from engaging in circumvention or interception with respect to DISH Network's security system or satellite signal, or assisting others in the same. Both the Communications Act and the DMCA permit courts to grant permanent injunctions to prevent further statutory violations. 47 U.S.C. § 605(e)(3); 17 U.S.C. § 1203(b)(1).

A party seeking a permanent injunction must show: "(1) that it has suffered an irreparable injury; (2) that remedies available at law, such as monetary damages, are inadequate to compensate for that injury; (3) that, considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and (4) that the public interest would not be disserved by a permanent injunction." *Autodesk, Inc. v. Flores*, No. 10-CV-01917-LHK, 2011 WL 337836, at *6 (N.D. Cal. Jan. 31, 2011) (citing *eBay Inc. v. MercExchange, L.L.C.*, 547 U.S. 388, 391 (2006)).

Here, Plaintiffs contend that they have suffered irreparable damage to their reputation and that significant revenues have been diverted from DISH Network as a result of Defendant's conduct. *See Coxcom, Inc. v. Chaffee*, 536 F.3d 101, 112 (1st Cir. 2008) (upholding district court grant of permanent injunction in light of the difficulty in measuring lost revenue from pay-per-view service). With respect to the third and fourth factors, an injunction would do no more than require Defendant to comply with federal and state anti-piracy laws, and "the public has an interest in the enforcement of . . . statutes." *Id.* at 112.; *See Sec. Indus. Ass'n v. Bd. of Governors of Fed. Reserve Sys.*, 628 F.Supp. 1438, 1443 (D.D.C.1986). Plaintiffs' request for injunctive relief is sufficiently tailored to prevent only the offending conduct at issue in this case. Accordingly, the Court concludes that Plaintiffs are entitled to a permanent injunction consistent with their request.

IV. ORDER

Good cause therefor appearing, the motion for summary judgment will be GRANTED. Plaintiffs will be awarded statutory damages in the amount of $2,250,600, and a permanent injunction will issue. Plaintiffs also shall recover their attorneys' fees and expenses reasonably

13

incurred in prosecuting Defendant's violation of the DMCA and Communications Act. Counsel for Plaintiffs shall file a declaration itemizing such fees and expenses within seven (7) days from the date of this order. The Clerk of the Court shall enter judgment and close the file.

IT IS SO ORDERED.

DATED: March 9, 2011

_____
JEREMY FOGEL
United States District Judge