UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

DISH NETWORK, L.L.C., *et al.*, Plaintiffs, v. VICXON CORPORATION, *et al.*, Defendants.	Case No. 12-cv-9-L(WVG) **ORDER GRANTING PLAINTIFFS' UNOPPOSED MOTION FOR SUMMARY JUDGMENT [DOC. 57]**

On January 3, 2012, Plaintiffs DISH Network, L.L.C., EchoStar Technologies L.L.C. ("EchoStar"), and NagraStar L.L.C. filed their complaint against Defendants Vicxon Corporation, a Korean corporation, and Soo Jong Yeo, a Korean citizen, alleging violations of the Digital Millennium Copyright Act ("DMCA"), the Federal Communications Act ("FCA"), and the Electronic Communications Privacy Act ("ECPA"). Now pending before the Court is Plaintiffs' unopposed motion for summary judgment.

The Court found the motion suitable for determination on the papers submitted and without oral argument. *See* Civ. L.R. 7.1(d.1). (Doc. 58.) For the following reasons, the Court **GRANTS** Plaintiffs' motion for summary judgment. (Doc. 57.)

//

I. BACKGROUND

A. Plaintiffs' Subscription-Based Satellite TV Programming

DISH Network, EchoStar, and NagraStar operate various elements of the DISH Network satellite television distribution system. DISH Network is a multi-channel provider that delivers video, audio, and data services via a direct broadcast satellite system to authorized subscribers throughout the United States. (Duval Decl. ¶ 4 [Doc. 57-2].) EchoStar designs, develops, and distributes receiver systems, satellite dishes, and other digital equipment for use in the DISH Network system. (*Id.* ¶ 9.) NagraStar provides DISH Network with "smart cards" that are used in EchoStar's satellite receivers to facilitate the decryption of DISH Network's programming signals. (*Id.* ¶ 13.)

DISH Network contracts for and purchases the distribution rights for the copyrighted programming it broadcasts from outlets such as network affiliates, cable networks, motion-picture distributors, sports leagues, event promoters, and other holders of programming rights. (Duval Decl. ¶ 6.) It uses high-powered satellites to broadcast, among other things, movies, sports, and general entertainment services 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. (*Id.* ¶ 5.) DISH Network then digitally encodes and scrambles the broadcast signals using NagraStar's encryption technology, and delivers the scrambled signals via satellite to the EchoStar dishes and receivers owned or leased by authorized subscribers. (*Id.* ¶ 8.)

Plaintiffs use an encryption system to restrict access to their signals such that only authorized subscribers can decrypt the signals. (*See* Duval Decl. ¶ 11.) To effectuate this decryption system, Plaintiffs use smart cards that carry a secured embedded microprocessor provided by NagraStar. (*Id.* ¶¶ 9, 12.) The microprocessor contains information that provides instructions and commands to the smart card in the everyday operation of the NagraStar security system as well as decryption keys. (*Id.* ¶ 12.) The EchoStar receiver possesses an incoming DISH Network satellite signal by locating an encrypted part of the transmission, known as the entitlement control message, and then forwards that message to the smart card. (*Id.* ¶ 13.) If the

subscriber is tuned to a channel he is authorized to watch, the smart card uses its decryption keys to unlock the message, uncovering a control word. (*Id.*) The control word is then transmitted back to the receiver in order to decrypt the DISH Network satellite signal. (*Id.*) Then the receiver and smart card convert DISH Network's encrypted satellite signal into viewable programming that can be displayed on the attached television of an authorized DISH Network subscriber. (*Id.*)

B. Piracy of DISH Network Programming Using Free-To-Air Receivers

Satellite television pirates have developed several means of circumventing the DISH Network security system and intercepting DISH Network satellite broadcasts using Free-To-Air ("FTA")[1] satellite receivers. (Duval Decl. ¶ 15.) In one method of circumvention, the pirates created software which was programmed onto the FTA receiver so as to mimic a DISH Network smart card. (*Id.* ¶¶ 15–16.) Once the FTA receivers were programmed with the card-hack software, the "modified" receiver could decrypt DISH Network's signals without authorization. (*Id.* ¶ 16.) This method requires the piracy software to be regularly updated in order to overcome countermeasures employed by DISH Network, such as changing the decryption keys required to access proprietary information. (*Id.* ¶ 17.)

Recently, pirates have developed a new method of obtaining DISH Network's signals without authorization called Internet Key Sharing ("IKS"). (Duval Decl. ¶ 18.) IKS uses internet-enabled FTA receivers. (*Id.* ¶ 19.) In IKS piracy, the decoding keys that allow the decryption of DISH Network's signals are captured from a computer server ("IKS server") that connects with multiple subscribed NagraStar smart cards. (*Id.* ¶ 20.) Control words obtained from the authorized smart cards are sent from the IKS server over the internet to unauthorized receivers, where they are used to decrypt DISH Network's satellite signal and view its

[1] FTA satellite receivers were originally designed to receive free satellite television channels that carry unencrypted programming. FTA programming is mostly limited to ethnic, religious, business, music, information, or advertising content, rather than the subscription-based content offered by satellite providers such as DISH Network.

programming without paying the subscription fee. (*Id.*) In short, IKS servers allow the decoding keys to be shared over the internet such that internet-enabled FTA receivers programmed with modified FTA/IKS piracy software can use these decoding keys to decrypt DISH Network's signals without authorization. Furthermore, because IKS is based on the trafficking of control words obtained from subscribed DISH Network receiving equipment, this method of satellite piracy remains effective even after DISH Network's transition to "Nagra 3," the latest generation security technology that was recently introduced by NagraStar. (*Id.* ¶ 21.)

C. Evidence of Defendants' Distribution of Piracy Devices and Piracy Software

1. Vicxon Corporation and Soo Jong Yeo

Vicxon is the exclusive manufacturer of Sonicview-branded satellite receivers and add-on dongles. (Yeo Decl. ¶ 8 [Doc. 33-2].) Plaintiffs previously filed suit against Sonicview USA, Inc. for the distribution of the equipment manufactured by Vicxon. This Court granted Plaintiffs' motion for summary judgment in that action. *See DISH Network, L.L.C. v. Sonicview USA, Inc.*, No. 09-CV-1553-L WVG, 2012 WL 1965279 (S.D. Cal. May 31, 2012). Vicxon manufactures receivers and dongles, referred to as iHubs, for Sonicview. The receivers include the following models: SV-HD8000, SV-360 Elite, SV-360 Premier, and SV-4000. From January 2009 to August 2009, Vicxon distributed at least 111,291 receivers to Sonicview, consisting of 27,500 SC-360 Elites, 84,910 SV-360 Premiers, and 8,881 SV-HD8000s. (Hagan Decl. ¶¶ 6–7, Ex. 5.) From May 2009 to August 2009, Vicxon distributed at least 17,500 iHubs to Sonicview USA. (*Id.* ¶¶ 6, 8.)

Mr. Yeo is the President and Chief Executive Officer of Vicxon. (Yeo Decl. ¶ 8.) Sonicview dealt exclusively with Mr. Yeo as the main point of contact at Vicxon, and ordered Sonicview-branded products solely from him. (Sanz Dep. 73:13–74:5.) Mr. Yeo visited California multiple times to conduct business with Sonicview, and served as the lead in marketing and giving product demonstrations of Sonicview recievers and iHubs during his visits. (Yeo Decl. ¶ 30.) Additionally, all of Vicxon's invoices to Sonicview were endorsed with Mr. Yeo's signature. (Second Yeo Decl. ¶ 3 [Doc. 42-1]; Hagan Decl. ¶ 6, Ex. 5.)

2. Expert Analysis of Vicxon's Devices

a. Vicxon's Receivers and iHubs, and the A-1 Modules

Plaintiffs' expert, Dr. Aviel Rubin, through his company Independent Security Evaluators ("ISE"), analyzed a sample of Sonicview-branded receivers' factory firmware for the models SV-HD8000, SV-360 Elite, and SV-360 Premier. (Rubin Decl. ¶¶ 1–3.) Each model analyzed contained more than one exact match of the proprietary code and data that resides on Plaintiffs' smart card, a particular algorithm important for encrypting and decrypting DISH Network satellite signals, and a graphical user interface. (*Id.* ¶¶ 5–8.) There were strong similarities between the Sonicview-branded receivers' firmware and that of existing piracy firmware. (*Id.* ¶ 9.) Dr. Rubin concluded that Sonicview-branded receivers "have multiple elements that serve no legitimate purpose or use in a receiver intended solely for [FTA] applications," and all of these elements are related to piracy of the DISH Network satellite signal. (*Id.* ¶ 10.) Furthermore, Dr. Ruben concluded that strong similarities exist between the factory and pirate versions of the Sonicview receiver firmware, suggesting a cooperative relationship between the factory and pirate firmware developers. (*Id.*)

Another expert, Nigel Jones, through his company R.M.B. Consulting ("R.M.B."), analyzed the Sonicview-branded iHub and A-1 module in conjunction with Sonicview-branded receivers. (Jones Decl. ¶ 2.) According to Mr. Jones, the iHub is a serial Ethernet adapter promoted by Sonicview for use with its receivers in order to automatically update receiver firmware, download images and music, and play games. (*Id.* ¶ 4.) However, the iHub lacks software support for firmware updates, and it is particularly impractical for such updates because it costs around $100 per device and updates are infrequent. (*Id.* ¶ 6.) The iHub is also impractical for downloading images and music, and for playing interactive games because of its low bandwidth. (*Id.* ¶ 7.) It comes with a 16-digit code that enables the Sonicview-branded receiver to access the IKS server through the dongle, which in turn allows for the piracy of DISH Network programming when loaded with the piracy software. (*Id.* ¶ 9.) For the Sonicview piracy software to make access to the IKS server contingent on entry of a valid iHub code, the developers of the piracy software and the persons responsible for the IKS server must have a list

of valid iHub codes. (*Id.*) Thus, Mr. Jones concluded that "the iHub is designed for and has no practical use other than DISH Network piracy," and "the suppliers of iHub are working closely with the persons responsible for Sonicview receiver piracy software and the IKS server supporting Sonicview receivers." (*Id.* ¶ 10.)

When Mr. Jones analyzed the A-1 module, he found that the module works in conjunction with SV-HD8000—when loaded with piracy software—to receive DISH Network's high-definition programing. (Jones Decl. ¶ 14.) The A-1 module contains same principal integrated circuit, the Broadcom BCM4500 demodulator, as the set-top boxes supplied by EchoStar for the DISH Network system. (*Id.* ¶¶ 11, 13.) Mr. Jones concluded that "the A-1 module is designed to receive DISH Network's high-definition programming, and has no legitimate commercial purpose or use," and that "the A-1 module and Sonicview receivers are originating from a common supplier." (*Id.* ¶ 16.) He further concluded that the SV-HD8000, SV-360 Elite, SV-360 Premier, iHub, and A-1 module are each designed, produced and may be used for circumventing the DISH Network security system and receive DISH Network programming without authorization. (*Id.*)

b. The Piracy Software

Sonicview operated www.sonicviewusa.com, which contained piracy software—software intended for use with Sonicview-branded receivers to decrypt DISH Network's satellite television programming—available for download. (*See* Rogers Decl. ¶¶ 1, 6.) Vicxon provided the piracy software to Sonicview to post on their website. (Sanz Dep. 118:17–119:2; 123:7–124:25.) These piracy software files were made available for download after certain Sonicview-branded receiver models were mentioned on the website. (McMullen Decl. ¶¶ 8–10.) A NagraStar security technician tested at least one Sonicview-branded receiver by loading it with the corresponding piracy software downloaded from Sonicview's website. (*Id.* ¶ 8.) He found that the piracy software enabled the receiver to circumvent the NagraStar security system and receive DISH Network programming. (*Id.* ¶ 10.)

//

On January 3, 2013, Plaintiffs commenced this action. In the complaint, they assert six claims against all defendants for: (1) violation of the DMCA, 17 U.S.C. § 1201(a)(1); (2) violation of the DMCA, 17 U.S.C. §§ 1201(a)(2) & (b)(1); (3) violation of the FCA, 47 U.S.C. § 605(a); (4) violation of the FCA, 47 U.S.C. § 605(e)(4); and (5) violation of the ECPA, 18 U.S.C. § 2511(1)(a). On June 12, 2013, Plaintiffs filed a motion for summary judgment. (Doc. 57.) To date, Defendants have not opposed the motion.

II. LEGAL STANDARD

Summary judgment is appropriate under Rule 56(c) where the moving party demonstrates the absence of a genuine issue of material fact and entitlement to judgment as a matter of law. *See* Fed. R. Civ. P. 56(c); *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986). A fact is material when, under the governing substantive law, it could affect the outcome of the case. *Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986); *Freeman v. Arpaio*, 125 F.3d 732, 735 (9th Cir. 1997). A dispute about a material fact is genuine if "the evidence is such that a reasonable jury could return a verdict for the nonmoving party." *Anderson*, 477 U.S. at 248.

A party seeking summary judgment always bears the initial burden of establishing the absence of a genuine issue of material fact. *Celotex*, 477 U.S. at 323. The moving party can satisfy this burden in two ways: (1) by presenting evidence that negates an essential element of the nonmoving party's case; or (2) by demonstrating that the nonmoving party failed to make a showing sufficient to establish an element essential to that party's case on which that party will bear the burden of proof at trial. *Id.* at 322-23. "Disputes over irrelevant or unnecessary facts will not preclude a grant of summary judgment." *T.W. Elec. Serv., Inc. v. Pac. Elec. Contractors Ass'n*, 809 F.2d 626, 630 (9th Cir. 1987).

//

//

//

//

//

"The district court may limit its review to the documents submitted for the purpose of summary judgment and those parts of the record specifically referenced therein." *Carmen v. San Francisco Unified Sch. Dist.*, 237 F.3d 1026, 1030 (9th Cir. 2001). Therefore, the court is not obligated "to scour the record in search of a genuine issue of triable fact." *Keenan v. Allen*, 91 F.3d 1275, 1279 (9th Cir. 1996) (citing *Richards v. Combined Ins. Co. of Am.*, 55 F.3d 247, 251 (7th Cir. 1995)). If the moving party fails to discharge this initial burden, summary judgment must be denied and the court need not consider the nonmoving party's evidence. *Adickes v. S.H. Kress & Co.*, 398 U.S. 144, 159-60 (1970).

If the moving party meets this initial burden, the nonmoving party cannot defeat summary judgment merely by demonstrating "that there is some metaphysical doubt as to the material facts." *Matsushita Electric Indus. Co., Ltd. v. Zenith Radio Corp.*, 475 U.S. 574, 586 (1986); *Triton Energy Corp. v. Square D Co.*, 68 F.3d 1216, 1221 (9th Cir. 1995) ("The mere existence of a scintilla of evidence in support of the nonmoving party's position is not sufficient.") (citing *Anderson*, 477 U.S. at 242, 252). Rather, the nonmoving party must "go beyond the pleadings" and by "the depositions, answers to interrogatories, and admissions on file," designate "specific facts showing that there is a genuine issue for trial.'" *Celotex*, 477 U.S. at 324 (quoting Fed. R. Civ. P. 56(e)).

When making this determination, the court must view all inferences drawn from the underlying facts in the light most favorable to the nonmoving party. *See Matsushita*, 475 U.S. at 587. "Credibility determinations, the weighing of evidence, and the drawing of legitimate inferences from the facts are jury functions, not those of a judge, [when] he [or she] is ruling on a motion for summary judgment." *Anderson*, 477 U.S. at 255.

III. DISCUSSION

A. Liability Under the Digital Millennium Copyright Act

Section 1201(a)(2) of the Digital Millennium Copyright Act prohibits "manufactur[ing], import[ing], 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). In order to establish liability under this section, plaintiffs need only establish that defendants violated one of the three prongs. *See* 17 U.S.C. § 1201(a)(2). Moreover, potential lawful or fair use is not a defense to § 1201(a) when its requirements are established. *See Realnetworks, Inc. v. DVD Copy Control Ass'n*, 641 F. Supp. 913, 942 (N.D. Cal. 2009); *Sony Computer Entm't Am., Inc. v. Divineo, Inc.*, 457 F. Supp. 2d 957, 965 (N.D. Cal. 2006) ("[D]ownstream customers' lawful or fair use of circumvention devices does not relieve [the defendant] from liability for trafficking of such devices under DMCA.").

Plaintiffs contend that Vicxon receivers and iHubs are designed and produced to circumvent DISH Network's security system, and used primarily for that purpose. (Pls.' Mot. 17:11–23:2 [Doc. 57-1].) To support their contention, Plaintiffs rely on the same evidence used in their action against Sonicview, including: (1) ISE's and R.M.B.'s expert reports that conclude that the Vicxon-manufactured receiver and iHub have several firmware and hardware components that serve limited or no legitimate purpose other than circumvention of DISH Network's security system; (2) R.M.B.'s determination that the receivers and corresponding piracy software originated from Vicxon; (3) the substantial number of piracy software downloads to support Sonicview recievers. (*See id.*)

Section 1201(a)(2) addresses products that circumvent a technological measure that effectively controls access to a copyrighted work. Under the statute, "'circumvent a technological measure' means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure without authority of the copyright owner." 17 U.S.C. § 1201(a)(3)(A). "[A] technological measure

'effectively controls access to a [copyrighted] work' if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." *Id.* § 1201(a)(3)(B). The undisputed evidence shows that Plaintiffs employed measures to control access to copyrighted works, and, as discussed further below, that Defendants manufactured receivers and dongles designed to circumvent Plaintiffs' security measures. Furthermore, Plaintiffs use complex security measures to prevent unauthorized access to the copyrighted programming that they broadcast, including encrypting the signals and providing equipment necessary for lawful users to decrypt the signals. (Duval Decl. ¶¶ 4–13.)

Plaintiffs also present evidence that shows that Defendants' receivers are designed and produced to circumvent Plaintiffs' security measures. Plaintiffs' experts found that the receivers are structurally altered to accommodate pirating devices, such as the iHub and A-1 module. The combination of a Sonicview receiver and iHub—both of which Vicxon manufactures—along with the A-1 module permits unauthorized access to DISH Network's satellite programming by circumventing Plaintiffs' security measures when loaded with the piracy software. If these items were manufactured individually, it is imaginable that it may simply be a mere coincidence that the these products are being used to avoid Plaintiffs' security measures. However, there is undisputed evidence that Vicxon supplied all of the necessary components—the piracy software, dongle and receiver—which in combination allows to access DISH Network's programing without permission.

Plaintiffs' evidence also shows that the Defendants' receivers and iHubs are primarily used for piracy. There have been more than 2.5 million downloads of the piracy software that is tailored to operate on Sonicview-branded receivers, and Vicxon has distributed at least 138,791 Sonicview recievers. Also, the receivers include proprietary information from DISH Network smart cards and a decryption algorithm used in DISH Network's security system that serve no legitimate purpose. Similarly, R.M.B. found that the iHub is impractical, if not unable, for use in any capacity when connected with a Sonicview receiver unless it is loaded with piracy software. From these facts, it is reasonable to infer that the receivers and iHubs served the limited purpose

of circumventing Plaintiffs' security measures. Thus, the Court concludes that Defendants also violated the second prong of § 1201(a)(2).

In sum, the Court finds the Defendants liable for violations of § 1201(a)(2).

B. Mr. Yeo's Individual Liability for Vicxon's Violations of the DCMA

The Ninth Circuit has held that "a corporate officer or director is, in general, personally liable for all torts which he authorizes or directs or in which he participates, notwithstanding that he acted as an agent of the corporation and not on his own behalf." *The Comm. for Idaho's High Desert, Inc. v. Yost*, 92 F.3d 814, 823 (9th Cir. 1996) (quoting *Transgo, Inc. v. Ajac Transmission Parts Corp.*, 768 F.2d 1001, 1021 (9th Cir. 1985)). The Ninth Circuit has also noted that "[c]ases which have found personal liability on the part of corporate officers have typically involved instances where the defendant was the 'guiding spirit' behind the wrongful conduct . . . or the 'central figure' in the challenged corporate activity." *Davis v. Metro Productions, Inc.*, 885 F.2d 515, 524 n.10 (9th Cir. 1989) (internal citations omitted). This principle has been by courts applied in copyright cases. *See e.g.*, *Bangkok Broad. & T.V. Co., Ltd. v. IPTV Corp.*, 742 F. Supp. 2d 1101, 1114 (C.D. Cal. 2010).

Plaintiffs contend that Mr. Yeo has been a "guiding spirit" and "central figure" in the trafficking of Sonicview receivers and iHubs, and therefore are liable for Vicxon's copyright infringement. (Pls.' Mot. 23:3–24:28.) They direct the Court to the fact that Mr. Yeo, in his position as Chief Executive Officer and President of Vicxon, participated in running Vicxon's day-to-day operations, such as selling products to Sonicview, endorsing invoices to Sonicview, and visiting California on multiple occasions to conduct business with Sonicview. (*Id.* at 24:1–10.) These are uncontroverted facts that demonstrate Mr. Yeo is the "guiding spirit" behind Vicxon's activities, including Vicxon's production of piracy devices and software. Accordingly, the Court finds Mr. Yeo individually liable for the Sonicview receivers and iHubs distributed by his company in violation of the DMCA.

//

//

C. Statutory Damages Under the DMCA

The DMCA provides for "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." *Id.* § 1203(c)(5)(A); *see also Peer Int'l Corp. v. Pausa Records, Inc.*, 909 F.2d 1332, 1336 (9th Cir.1990) ("[T]he court has wide discretion in determining the amount of statutory damages to be awarded, constrained only by the specified maxima and minima."). Courts may award statutory damages for each device sold. *Sony Computer Entm't America, Inc. v. Filipak*, 406 F. Supp. 2d 1068, 1074. (N.D.Cal.2005) ("[Section] 1203(c)(3)(A) authorizes a separate award of statutory damages for each device sold"); *Craigslist, Inc. v. Naturemarket, Inc.*, 694 F. Supp. 2d 1039, 1064 (N.D.Cal.2010) (treating each unit sold as a violation).

Plaintffs seek damages for the number of devices—including receivers and iHubs—distributed by Defendants. This calculation of damages amounts to $27,758,200 for the at least 138,791 Sonicview receivers and iHubs distributed in violation of the DMCA at $200 per device. (Pls.' Mot. 26:10–21.) The evidence establishing the numbers associated with the devices distributed is undisputed, and that consequently establishes Vicxon's DCMA violations. Plaintiffs reasonably request the statutory minimum, and are not seeking damages for Vicxon's distribution of piracy software. Accordingly, the Court awards Plaintiffs $27,758,200 in statutory damages against Defendants. *See* 17 U.S.C. § 1203(c)(3)(A).

D. Permanent Injunction

Plaintiffs seek a permanent injunction enjoining Defendants' unlawful conduct. Section 1203(b)(1) of the DMCA authorizes the Court to "grant . . . permanent injunctions on such terms as it deems reasonable to prevent or restrain a violation." The Court finds that under the facts of this case, Plaintiffs are entitled to a permanent injunction.

Defendants are enjoined from:

- manufacturing, importing, offering to the public, or otherwise trafficking in Sonicview receivers, iHubs, software files, or any other technology or part thereof used in circumventing Plaintiffs' security system or intercepting Plaintiffs' programming;
- circumventing or assisting others in circumventing Plaintiffs' security system, or otherwise intercepting or assisting others in intercepting Plaintiffs' signal;
- testing, analyzing, reverse engineering, manipulating, or otherwise extracting codes, data, or information from Plaintiffs' satellite receivers, smart cards, satellite data stream, or any other part or component of Plaintiffs' security system.

Additionally, Defendants are ordered to destroy all Sonicview-branded receivers, iHubs, and piracy software in their possession in accordance with 17 U.S.C. § 1203(b)(6). *See Autodesk, Inc. v. Flores*, No. 10-CV-1917-LHK, 2011 WL 337836, at *11 (N.D. Cal. Jan. 31, 2011).

IV. CONCLUSION & ORDER

In light of the foregoing, the Court **GRANTS** Plaintiffs' unopposed motion for summary judgment. (Doc. 57.) The Clerk of the Court shall enter a judgment in favor of Plaintiffs in the amount of $27,758,200 against Defendants. Furthermore, Defendants are also permanently enjoined as described above, and ordered to destroy all Sonicview receivers, iHubs, and piracy software in their possession.

IT IS SO ORDERED.

DATED: July 25, 2013

M. James Lorenz
United States District Court Judge