



3. As a result of Defendants' failure to answer, or otherwise appear in this action, the Court accepts as true the following well-pleaded allegations in Nagraivision's amended complaint:

a. Nagraivision provides security technology to several prominent broadcasters in the pay-television industry, which ensures secure access to their subscription-based television services. Nagraivision's customers serve markets globally, including DISH Network in the United States and Telefonica and Claro TV Brazil in Latin America. (Am. Compl. ¶¶ 12, 22.)

b. Pay-television broadcasters that use the security technology of Nagraivision transmit their signal to subscribers in an encrypted format. To receive the signal, subscribers are required to purchase or lease from the broadcaster a receiver paired with a smart card, along with a programming subscription package. Viewing rights vary based on the services purchased from the pay-television broadcaster. (*Id.* ¶ 13.)

c. Nagraivision designs and licenses software incorporated into the receivers and smart cards, and also manufactures smart cards. The smart card is used to (i) manage, store, and communicate to the receiver the subscriber's right to decrypt specific channels based on his subscription plan, and (ii) decrypt the encrypted control words or "keys" required to unlock and view the channels for which the subscriber has purchased access. (*Id.* ¶ 14.)

d. Nagraivision's control words are transmitted to subscribers in the encrypted audio and video streams of the pay-television broadcaster. Control words are channel specific and change automatically about every few seconds. The control words are double protected by being delivered in encrypted packets called "entitlement control messages" ("ECMs"). The keys used to decrypt ECMs, called "transmission keys", are stored in the subscriber's smart card. (*Id.* ¶ 15.)

e. When a subscriber wants to view a specific channel, the receiver obtains the ECM containing the encrypted control word and forwards it to the smart card. The smart card uses its current transmission key to decrypt the ECM. The smart card then looks in its rights database to confirm the subscriber purchased a subscription to view the programming the control word will

decrypt. If the rights match, the smart card forwards the unencrypted control word to the receiver, where the control word decrypts the broadcast. (*Id.* ¶ 16.)

f. “Internet key sharing” (“IKS”) is a form of pay-television piracy involving unauthorized harvesting and redistribution of Nagravision’s control words. Nagravision’s control words are obtained by purchasing a subscription with the pay-television broadcaster, and using a genuine smart card activated on that subscription to decrypt ECMs containing the control words. Once decrypted, control words are sent from the smart card to a computer server, called an “IKS server”, where they are saved in the server’s memory or cache. (*Id.* ¶ 17.)

g. Nagravision control words are distributed from the IKS server to end users. End users access the IKS server with an unauthorized receiver connected to the Internet. When the end user tunes to a channel, the unauthorized receiver requests the control word for that channel from the IKS server. The IKS server sends the control word over the Internet to the unauthorized receiver, allowing the end user to decrypt the channel without purchasing a subscription from the pay-television broadcaster. (*Id.* ¶ 18.)

h. Defendants manufacture and distribute unauthorized receivers under brand names including Globalsat, AZAmerica, NAZABox, Captiveworks, and Limesat, among them the Globalsat GS-111 and GS-300, AZAmerica S1005, NAZABox NZ S-1010, Captiveworks CW-600S, CW-650S, CW-700S, CW-800S, 900 HD, and Limesat Ultra. (*Id.* ¶ 21.)

i. Defendants’ Globalsat, AZAmerica, and NAZABox receivers are capable of circumventing Nagravision’s security system and intercepting the subscription-based television programming provided by Nagravision’s customers in Latin America, Telefonica and Claro TV Brazil. Defendants’ Limesat and Captiveworks receivers can be used to circumvent Nagravision’s security system and intercept the subscription-based television programming of DISH Network, which is Nagravision’s customer in the United States. Defendants imported and sold Limesat and Captiveworks receivers to distributors located in the United States. (*Id.* ¶¶ 22, 28.)

j. Defendants' unauthorized receivers contain multiple hardware and software components that are unnecessary for receiving unencrypted satellite broadcasts, but are essential for decrypting broadcasts protected by the Nagravision security system. The components include proprietary Nagravision code taken from the ROM and EEPROM of a pay-television provider's smart card, decryption keys and a decryption algorithm used in Nagravision's security system, and other design elements relating to pay-television piracy. (*Id.* ¶¶ 23, 29-30.)

k. Defendants operate an IKS service from servers located in the United States that are used to distribute Nagravision's control words to end users of their Globalsat, AZAmerica, and NAZABox receivers. The servers involved are: (i) "authentication servers", which confirm the end user is permitted to access the IKS service and provide information to connect to additional servers that deliver Nagravision's control words; and (ii) "control word servers", which function as a cache by storing Nagravision's control words and also a front end by transmitting the control words from the cache to end users requesting control words through their unauthorized receiver. Defendants developed the control word sharing technology and assembled the IKS servers used to support their IKS service. (*Id.* ¶¶ 24-26, 32, 38.)

l. Defendants' control word sharing technology, services, and unauthorized receivers are primarily designed and produced to circumvent Nagravision's security technology, have no commercially significant purpose or use other than circumventing Nagravision's security technology, and are primarily of assistance in the unauthorized decryption of satellite television broadcasts protected by Nagravision's security technology. Defendants assisted others to receive Nagravision's control words and satellite television broadcasts protected by Nagravision's security technology, without authorization and for their own benefit, by having provided IKS services and unauthorized receivers. (*Id.* ¶ 33, 39, 43.)

m. Defendants intended for their control word sharing technology, services, and receivers to be used in the unauthorized decryption of satellite television broadcasts protected

by Nagravision's security technology, or at least knew or should have known that the foregoing are primarily used for this purpose. (*Id.* ¶¶ 35, 40, 44.)

n. Defendants' acts violate the Digital Millennium Copyright Act ("DMCA"), 17 U.S.C. § 1201(a)(2), and the Federal Communications Act ("FCA"), 47 U.S.C. §§ 605(e)(4) and 605(a), as alleged in Counts I, II and III of Nagravision's amended complaint. (*Id.* ¶¶ 31-45.)

o. Nagravision elected to recover statutory damages in the amount of \$200 for each of Defendants' violations of the DMCA. The damages sought by Nagravision are at the very bottom of the range authorized by 17 U.S.C. §1203(c)(3)(A), substantially less than the \$10,000 per violation statutory minimum allowed by the FCA, in line with statutory damages awarded in similar cases, and reasonable given Defendants' misconduct. Nagravision submitted evidence that Defendants provided their IKS services to at least 501,985 end users, and distributed at least 7,274 Limesat and Captiveworks receivers, for a combined total of 509,259 violations of the DMCA.

## II. FINAL JUDGMENT AND PERMANENT INJUNCTION

Upon default of Defendants, and having reviewed the record, evidence, and applicable law in this matter, the Court hereby ORDERS as follows:

1. Defendants, and any of their officers, agents, servants, employees, or other persons acting in active concert or participation with any of the foregoing that receives actual notice of the order, is permanently enjoined from:

a. Manufacturing, importing, assembling, selling, distributing, offering to the public, providing, or trafficking in: (a) any product, technology, or service used in acquiring or distributing Nagravision's control words; (b) Limesat receivers; (c) Captiveworks receivers; or (d) any other service, technology, product, equipment, device, component, or part thereof that:

i. is primarily designed or produced for circumventing Nagravision's security system or any other technological measure deployed by Nagravision that controls access to, copying, or distribution of copyrighted works;

ii. has only a limited commercially significant purpose or use other than to circumvent Nagravision's security system or any other technological measure deployed by Nagravision that controls access to, copying, or distribution of copyrighted works;

iii. is marketed for use in circumventing Nagravision's security system or any other technological measure deployed by Nagravision that controls access to, copying, or distribution of copyrighted works; or

iv. is primarily of assistance in the unauthorized decryption of direct-to-home satellite services protected by the Nagravision security technology.

b. Receiving or assisting others in receiving Nagravision's control words or satellite transmissions of television programming protected by Nagravision's security technology without authorization.

2. Third parties providing any form of web, server, domain registration, file hosting, or content delivery network services used by Defendants in connection with any of the activities enjoined in paragraph 1, and who receive actual notice of this Order, are enjoined from providing such services to Defendants in connection with any of the activities enjoined under paragraph 1.

3. Judgment is entered in favor of Nagravision on Counts I through III of the amended complaint, which allege violations of the DMCA, 17 U.S.C. § 1201(a)(2), and FCA, 47 U.S.C. §§ 605(e)(4) and 605(a).

4. In accordance with 17 U.S.C. § 1203(c)(3)(A), statutory damages of \$101,851,800 are awarded to Nagravision. The statutory damages are calculated based on Defendants' 509,259 violations of section 1201(a)(2) of the DMCA at \$200 per violation.

5. In accordance with 17 U.S.C. § 1203(b)(2), Defendants, and any of their officers, agents, servants, employees, or other persons acting in active concert or participation with any of the foregoing that receives actual notice of the order, must turn over for impoundment all items listed in paragraph 1(a), and any source code or other components of the receivers that incorporate

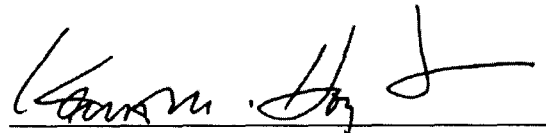
any portion of Nagravision's security technology. The items must be delivered to Nagravision's counsel of record no later than five court days following service of this order.

6. In accordance with 17 U.S.C. § 1203(b)(6), all items that Nagravision receives pursuant to paragraph 5 may be destroyed. Destruction may commence after the time for filing an appeal from this order has passed, provided that no such appeal has been filed.

7. The registries and registrars holding or listing the domain names gotechcn.com and goosat.com, upon receiving actual notice of this Order, shall (i) temporarily disable the domain names through a registry hold or otherwise, and make them inactive and non-transferable; and (ii) transfer these domain names to Nagravision, including changing the registrar of record to the registrar selected by Nagravision.

8. The Court retains jurisdiction over this action for a period of two years for purposes of enforcing this final judgment and permanent injunction.

SIGNED on this 18<sup>th</sup> day of August, 2016.



Kenneth M. Hoyt  
United States District Judge