

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MINNESOTA**

DISH NETWORK L.L.C., a Colorado
Limited Liability Company, ECHOSTAR
TECHNOLOGIES L.L.C., a Texas Limited
Liability Company, and NAGRASTAR LLC,
a Colorado Limited Liability Company,

Plaintiffs,

v.

GUSTAV DOBOS, an individual, and DOES
1-10

Defendant.

Civil Case No.: 0:09-cv-03448-JNE-SRN

AGREED FINAL JUDGMENT AND PERMANENT INJUNCTION

I. INTRODUCTION AND NATURE OF THE CASE

1. Plaintiffs brought this action against Defendant Gustav Dobos (hereinafter “Defendant”) for unlawfully distributing and otherwise trafficking in devices, components, and/or technologies intended to facilitate the illegal and unauthorized reception and decryption of DISH Network’s subscription and pay-per-view television programming.

2. DISH Network is a multi-channel video provider, providing video, audio, and data services to customers throughout the United States, Puerto Rico, and the U.S. Virgin Islands via a Direct Broadcast Satellite (“DBS”) system. DISH Network uses high-powered satellites to broadcast, among other things, movies, sports, and general entertainment services (“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).

3. To provide customers with a variety of Programming channels, DISH Network

continues to contract with and purchase the distribution rights of copyrighted Programming from providers such as network affiliates, pay and specialty broadcasters, cable networks, motion picture distributors, sports leagues, event promoters, and other content providers including without limitation, HBO, ESPN, SHOW Time, Cinemax and Disney among others.

4. Because DISH Network generates revenues through the sale of subscription packages and pay-per-view programming, and because the ability to attract and retain the distribution rights for Programming is dependent upon preventing the unauthorized reception of DISH Network Programming signals, all of DISH Network's video channels, except for certain promotional channels, are digitally secured and encrypted.

5. Plaintiffs protect their DISH Network Programming from unauthorized viewing by using a management and security system ("Security System"), which serves two interrelated functions: (1) subscriber-management—allowing DISH to "turn on" or "turn off" Programming that a customer ordered, cancelled, or changed; and (2) encryption—preventing individuals or entities who have not purchased DISH Network Programming from viewing it.

6. The Security System is comprised of two parts. First, DISH Network encrypts (electronically scrambles) its satellite signals using proprietary technology provided by NagraStar. Essentially, NagraStar provides DISH Network with "smart cards" ("Access Cards") that contain a microprocessor component that functions as a security computer to a "conditional access system" known as Digital Nagra Advanced Security Process ("DNASP"). These Access Cards and related encryption technology are utilized in the satellite receivers that customers either purchase or lease. Second, the DNASP uses a complex encryption system that is combined with a Digital Video Broadcasting ("DVB") scrambler/encoding system to effectively protect and encrypt DISH Network Programming.

7. Defendant violated federal laws by offering to the public, providing, or otherwise engaging in the traffic of devices, components, and/or technologies that are primarily designed to circumvent and/or defeat Plaintiffs' Security System and ultimately facilitate the unauthorized reception of Plaintiffs' encrypted satellite signals and copyrighted DISH Network Programming. Such devices, components and/or technologies include: firmware and software designed or used for piracy in connection with FTA receivers, Internet Key Sharing, Control Word Sharing, distribution of data or code for use in piracy, and nFusion-branded FTA receivers. Defendant acknowledges and admits that each of the foregoing was primarily designed, marketed and used to facilitate piracy of satellite television programming.

II. FINAL JUDGMENT & PERMANENT INJUNCTION

Upon stipulation by the Parties, the Court, having reviewed the evidence and arguments in this matter hereby ORDERS and ADJUDGES as follows:

(1) Defendant and anyone acting in active concert or participation with, or at the direction or control of Defendant are hereby PERMANENTLY ENJOINED from:

(a) offering to the public, providing, or otherwise trafficking in any satellite television receivers or set-top-boxes, software, firmware, or any other device, component, or technology, or part thereof, through any means including Internet key sharing (also known as Control Word Sharing), that:

(i) is primarily designed or produced for the purpose of circumventing Plaintiffs' Security System, including the encryption and access control protection contained in the software on DISH Network Access Cards, or any other technological measure adopted by Plaintiffs that effectively

controls access to copyrighted television programming on the DISH Network platform;

(ii) has only a limited commercially significant purpose or use other than to circumvent Plaintiffs' Security System, including the encryption and access control protection contained in the software on DISH Network Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted television programming on the DISH Network platform;

(iii) is marketed by either Defendant and/or others acting in concert with Defendant for use in circumventing Plaintiffs' Security System, including the encryption and access control protection contained in the software on DISH Network Access Cards, or any other technological measure adopted by Plaintiffs that effectively controls access to copyrighted programming on the DISH Network platform; and

(b) assembling, modifying, selling, importing and/or distributing any satellite television receivers, set-top-boxes, software, firmware, or other device, technology or part thereof knowing or having reason to know that such device, technology or part thereof is primarily of assistance in the unauthorized decryption of direct-to-home satellite services through any means including any Internet Key Sharing (also known as Control Word Sharing);

(c) intercepting Plaintiffs' transmissions without Plaintiffs' authorization through any means including Internet Key Sharing (also known as Control Word Sharing);

(d) assisting others in intercepting Plaintiffs' satellite television transmissions without Plaintiffs' authorization through any means including Internet Key Sharing (also known as Control Word Sharing);

(e) Testing, analyzing, reverse engineering, manipulating or otherwise extracting codes or other technological information or data from Plaintiffs' satellite television receivers, access cards, data stream or any other part or component of Plaintiffs' security system or other technology used to gain access to DISH Network programming including through the use of Internet Key Sharing (also known as Control Word Sharing); and

(f) Operating any website or URL that markets, promotes, distributes or provides any information or discussion forums related to the products, devices, technology, codes, software, hardware, firmware or components thereof which Defendant is permanently enjoined from manufacturing, promoting, distributing or trafficking in pursuant to section (1)(a)-(e) above of this Final Judgment and Permanent Injunction.

(2) This Permanent Injunction takes effect immediately.

(3) Should Defendant breach any part of this Final Judgment or Permanent Injunction, he shall be subject to damages in the amount of \$110,000 for each such breach or violation, which is the maximum statutory damage permitted per violation under 47 U.S.C. § 605(e)(3)(C)(i)-(ii). For purposes of assessing damages under this section, each "device, product, file, technology or part or component thereof" that is distributed by Defendant or others acting in active participation or concert with Defendant in violation of this Final Judgment and Permanent Injunction shall constitute a separate and discrete violation. In the case of any

software, firmware or other file distributed or posted by Defendant or others acting in active participation or concert with Defendant, each time that software, firmware or other file is downloaded by an end-user shall constitute a separate and discrete “violation” for purposes of quantifying damages set forth in this section.

(4) The Court further ORDERS judgment in favor of Plaintiffs DISH Network L.L.C., EchoStar Technologies L.L.C. and NagraStar LLC on each of Plaintiffs’ claims under 17 U.S.C. § 1201, 47 U.S.C. § 605, and 18 U.S.C. § 2511, and for breach of contract (Counts 1-5 in Plaintiffs’ Complaint) in the aggregate amount of Twenty Million Dollars (\$ 20,000,000.00) as to Defendant.

(5) The Court retains jurisdiction over this action for the purposes of enforcing this Final Judgment and Permanent Injunction and adjudicating any disputes regarding the Parties’ underlying settlement agreement, including but not limited to disputes regarding the enforcement or scope of the settlement agreement.

(6) Each of the Parties is to bear its own costs and attorney's fees.

(7) This is a final judgment. Any and all relief not expressly granted herein is denied.

It is so ORDERED.

SIGNED and ENTERED this ____ day of _____, 2010.

United States District Court Judge

Respectfully submitted,

DATED: January 20, 2010

HAGAN NOLL & BOYLE LLC

By: s/ Chad M. Hagan

Chad M. Hagan (*pro hac vice*)
chad.hagan@hnbllc.com
Two Memorial City Plaza
820 Gessner, Suite 940
Houston, TX 77024
Telephone: (713) 343-0478
Facsimile: (713) 758-0146

And

**ANDERSON, HELGEN, DAVIS & NISSEN,
LLC**

By: s/ Henry M. Helgen, III

Henry M. Helgen, III
hmh@andersonhelgen.com
Resident Counsel for Plaintiffs
Minnesota Attorney Number #151075
150 South Fifth Street, Suite 3100
Minneapolis, MN 55402
Telephone: (612) 435-6342
Facsimile: (612) 435-6379

Attorneys for Plaintiffs

DATED: January 20, 2010

MADIA LAW LLC

By: s/ J. Ashwin Madia

J. Ashwin Madia, #0321187
345 Union Plaza
333 Washington Avenue North
Minneapolis, MN 55401
Phone: 612.349.2723
Fax: 612.349.2760
Email: jamadia@madialaw.com

Attorney for Defendant Gustav Dobos