

UNITED STATES DISTRICT COURT
DISTRICT OF PUERTO RICO

UNITED STATES OF AMERICA,

v.

[1] ALNARDO VAZQUEZ,
also known as "Naldo," also known as
"naldo.dish,"
[2] AWILDO JIMENEZ,
also known as "Wildo," also known as
"joselo626," also known as "wildo20,"
[3] HIGINIO LAMBOY,
also known as "Ingi,"
Defendants.

INDICTMENT

Criminal No. 18-670 (ADC)

Violations:

18 U.S.C. § 371

17 U.S.C. §§ 1201(a)(1)(A) and (a)(2)(A)

18 U.S.C. § 2

(Three Counts)

RECEIVED AND FILED
CLERK'S OFFICE
U.S. DISTRICT COURT
SAN JUAN, P.R.

2018 OCT 24 PM 5:

THE GRAND JURY CHARGES:

Count One

(Conspiracy to Circumvent Copyright Protection Systems, Infringe Copyrights, and Traffic
in Satellite Decryption Devices)

1. At all times relevant to this Indictment:

Relevant Individuals and Entity

a. Defendant ALNARDO VAZQUEZ, a/k/a "Naldo" and "naldo.dish,"
resided in or around Salinas, Puerto Rico, and was one of the two owners and operators of an entity
that provided pirated satellite television service to thousands of clients for private financial gain.
Defendant VAZQUEZ was an organizer and leader of the conduct described herein.

b. Defendant AWILDO JIMENEZ, a/k/a "Wildo," "joselo626," and
"wildo20," resided in or around Salinas, Puerto Rico, and was the other owner and operator of an
entity that provided pirated satellite television service to thousands of clients for private financial

gain. Defendant JIMENEZ was an organizer and leader of the conduct described herein.

c. Defendant HIGINIO LAMBOY, a/k/a "Ingi," resided in or around Mayaguez, Puerto Rico, and sold the entity's pirated satellite television service. Defendant LAMBOY also installed and repaired equipment utilized in the provision of the pirated satellite television service.

d. DISH Network, LLC ("DISH") is a company based in Englewood, Colorado that provides satellite television services pirated by Defendants.

Background and Relevant Terms

e. In order to provide its services, DISH purchases distribution rights for copyrighted programming from content providers, then converts that content into digital signals that are encrypted and delivered via satellite to legitimate subscribers who have paid for the right to view the signals.

f. Equipment is provided to DISH subscribers to receive and process the satellite television signal, which consists primarily of a satellite reception dish and a satellite receiver. Access to DISH's services is limited to paid subscribers through a smartcard that is installed in the customer's receiver, as well as by encryption that scrambles the DISH signal. These measures are designed to prevent unauthorized users from viewing the signal, even in the event they have a dish and receiver unit that can physically receive and process the signal.

g. Each receiver and smartcard is assigned a unique serial number that is used by DISH when activating the equipment to ensure the equipment only decrypts programming the

customer is authorized to receive as part of his or her subscription package and pay-per-view purchases. Provided that the subscriber is tuned to a channel he or she is authorized to watch, the smartcard uses its decryption keys to unlock the message, uncovering a decryption code referred to as a "control word." The control word is transmitted back to the receiver in order to decrypt the DISH satellite signal.

h. At least partly as a result of the electronic countermeasures taken by DISH against earlier forms of piracy, pirates began to develop a particular method of obtaining DISH's signals without authorization, known as Internet Key Sharing ("IKS"). In IKS piracy, pirates capture and obtain control words from smartcards associated with DISH accounts that the pirate maintains or otherwise accesses. Once a pirate has captured particular control words, he or she places the control words for the particular channels on a server connected to the Internet ("IKS server").

i. IKS end-users ("end-users") obtain certain satellite receivers programmed with special software that enables the receivers to make a direct-to-server connection over the Internet to an IKS server to access particular control words to accomplish unauthorized decryption. The end-users' unauthorized receivers then utilize the control words to decrypt DISH's satellite signals to obtain DISH's programming without authorization and without payment of a fee to DISH. Access to an IKS server is usually restricted so that an end-user must purchase a subscription from the pirate to gain access to the IKS server.

The Conspiracy

2. Beginning at a time unknown and continuing to on or about July of 2016, in the District of Puerto Rico, and elsewhere, defendants

**[1] Alnardo Vazquez,
[2] Awildo Jimenez, and
[3] Higinio Lamboy,**

did knowingly agree, combine, and conspire to commit offenses against the United States, that is:

a. To willfully and for purposes of private financial gain circumvent a technological measure that effectively controls access to a work protected under Title 17 of the *United States Code*, in violation of Title 17, *United States Code*, Sections 1201(a)(1)(A), and 1204(a)(1); and

b. To willfully and for purposes of private financial gain traffic in a technology, product, service, and device that was primarily designed and produced for the purpose of circumventing a technological measure that effectively controlled access to a work protected under Title 17 of the *United States Code*, in violation of Title 17, *United States Code*, Sections 1201(a)(2)(A), and 1204(a)(1); and

c. To willfully and for purposes of private financial gain infringe a copyright by reproducing and distributing, including by electronic means, at least ten copies of one or more copyrighted works, with a total retail value of more than \$2,500, during a 180-day period, in violation of Title 17, *United States Code*, Section 506(a)(1)(A), and Title 18, *United States Code*, Section 2319(b)(1);

d. To manufacture, assemble, modify, import, export, sell, and distribute any electronic, mechanical, and other devices and equipment, knowing and having reason to know that the device and equipment was primarily of assistance in the unauthorized decryption of satellite cable programming, and direct-to-home satellite services, in violation of Title 47, *United States Code*, Section 605(e)(4).

Object of the Conspiracy

3. The object of the conspiracy was for Defendants and others to enrich themselves by providing pirated satellite television service to thousands of clients for private financial gain.

Manner and Means of the Conspiracy

4. It was part of the conspiracy that Defendants, together with others, captured and obtained control words from smartcards associated with DISH accounts that they controlled.

5. It was further part of the conspiracy that Defendants, together with others, placed these control words associated with particular channels of DISH programming onto an IKS server under their control.

6. It was further part of the conspiracy that Defendants, together with others, provided satellite receivers to end-users. These receivers were programmed with special software that enabled the receivers to make a direct-to-server connection over the Internet to the IKS server under Defendants' control in order to access particular control words to accomplish unauthorized decryption. The end-users' unauthorized receivers then utilized the control words to decrypt DISH's satellite signals to obtain DISH's programming without authorization.

7. It was further part of the conspiracy that Defendants, together with others, collected “subscription” payments from these end-users, without DISH’s authorization and for their own private financial gain.

8. It was further part of the conspiracy that Defendants, together with others, installed and repaired these receivers, as well as related equipment used by end-users to obtain pirated satellite television service.

Overt Acts

9. In furtherance of the conspiracy and to effect its unlawful object, Defendants and others committed and caused to be committed the following overt acts in the District of Puerto Rico and elsewhere:

a. On or about November 11, 2014, Defendant VAZQUEZ transmitted to Defendant JIMENEZ, in Puerto Rico, a copy of a bill for Internet services at a location in Salinas, Puerto Rico.

b. On or about January 11, 2015, Defendant VAZQUEZ and Defendant JIMENEZ transmitted online messages to one another concerning the purchase of servers to operate the IKS piracy operation in Salinas..

c. On or about January 15, 2015, Defendant VAZQUEZ and Defendant JIMENEZ transmitted online messages to one another regarding the operation of the IKS servers in Salinas, Puerto Rico and an outage of local Puerto Rico service.

d. On or about January 22, 2015, Defendant VAZQUEZ and Defendant

JIMENEZ transmitted online messages to one another where they discuss “super dealer” accounts and the elimination of users that are re-sharing pirated service.

e. On or about January 30, 2015, Defendant VAZQUEZ and Defendant JIMENEZ transmitted online messages to one another concerning technical problems and other issues related to the operation of IKS piracy.

f. On or about February 7, 2015, Defendant VAZQUEZ and Defendant JIMENEZ transmitted online messages to one another in Puerto Rico regarding the purchase of routers and other equipment to utilize for IKS piracy.

g. On or about November 3, 2015, Defendants JIMENEZ and VAZQUEZ possessed a large amount of equipment related to pirated DISH satellite television service at a location in Salinas, Puerto Rico.

h. On or about November 5, 2015, Defendant JIMENEZ possessed a large amount of equipment related to pirated DISH satellite television service at his residence in Salinas, Puerto Rico.

i. On or about December 17, 2015, Defendant VAZQUEZ and Defendant Lamboy transmitted online messages to one another in Puerto Rico regarding the sale of IKS piracy equipment.

j. On or about January 25, 2016, Defendant VAZQUEZ and Defendant LAMBOY transmitted online messages to each other in Puerto Rico regarding the number of IKS clients and accounts managed by Defendant Vazquez

k. On or about July 6, 2016, Defendant LAMBOY possessed a large amount of equipment related to pirated DISH satellite television service at his residence in Mayaguez, Puerto Rico.

All in violation of Title 18, *United States Code*, Section 371.

Count Two
(Trafficking in Technology Designed to Circumvent Copyright Protection Systems)

The allegations contained in paragraphs one (1) through eight (8) above and all their subparts are hereby incorporated by reference.

Beginning at a time unknown, and continuing until on or about July of 2016, in the District of Puerto Rico and elsewhere, the defendants:

**[1] Alnardo Vazquez,
[2] Awildo Jimenez, and
[3] Higinio Lamboy**

did traffic, and attempt to traffic, for purpose of commercial advantage and private financial gain, in a technology, product, service, and device, specifically software, knowing that the technology, product, service, and device was primarily designed and produced for the purpose of circumventing a technological measure that effectively controls access to a copyrighted work protected under Title 17 of the *United States Code*, namely proprietary software designed to operate and function on a Dish Network Receiver. All in violation of Title 17, *United States Code*, §§ 1201(a)(2)(A), 1204(a)(1), and Title 18, *United States Code*, § 2.

Count Three
(Circumventing a Technological Measure that Protects a Copyrighted Work)

The allegations contained in paragraphs one (1) through eight (8) above and all their subparts are hereby incorporated by reference.

Beginning at a time unknown, and continuing until on or about July of 2016, in the District of Puerto Rico and elsewhere, the defendants,

**[1] Alnardo Vazquez,
[2] Awildo Jimenez, and
[3] Higinio Lamboy,**

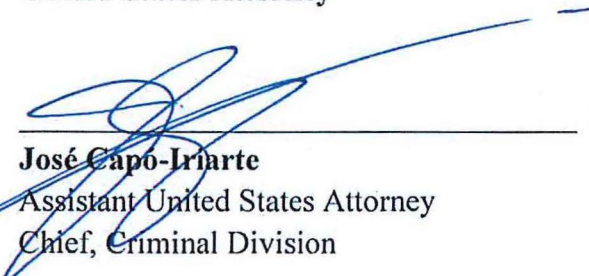
did willfully, and for purpose of commercial advantage and private financial gain, circumvent and attempt to circumvent a technological measure that effectively controls access to a work protected under Title 17 of the *United States Code*, namely proprietary software designed to operate and function on Dish Network Receiver. All in violation of Title 17, *United States Code*, §§ 1201(a)(1)(A), 1201(a)(1), and Title 18 *United States Code*, § 2.

[INTENTIONALLY BLANK]

TRUE BILL

ROSA EMILIA RODRIGUEZ-VELEZ
United States Attorney

FOREPERSON



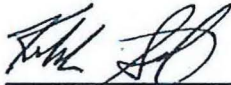
José Capo-Iriarte
Assistant United States Attorney
Chief, Criminal Division

Date:

Oct. 24, 2018



Nicholas W. Cannon
Assistant United States Attorney
Deputy Chief, Immigration, Cybercrimes, and
Child Exploitation



Kebharu Smith
Trial Attorney, Criminal Division