

NEWS RELEASE



OFFICE OF THE UNITED STATES ATTORNEY SOUTHERN DISTRICT OF CALIFORNIA

San Diego, California

***United States Attorney
Karen P. Hewitt***

For Further Information, Contact: Assistant U. S. Attorney Mitch Dembin, 619-557-5558

For Immediate Release

NEWS RELEASE SUMMARY - October 23, 2009

United States Attorney Karen P. Hewitt announced that Jung Kwak, also known as “Mr. Viewsat,” Phillip Allison, also known as “thebroken,” and Robert Ward, also known as “TDG” and as “thedssguy,” have tendered pleas of guilty to conspiring to violate the Digital Millennium Copyright Act. The three defendants were charged in a one-count indictment handed up by a federal grand jury sitting in San Diego on July 9, 2009.

In connection with their guilty pleas, the defendants admitted that beginning in or about March 2008, they determined to hire computer hackers to break the latest DISH Network encryption scheme, known as Nagra 3, so that the line of satellite receiver boxes sold by defendant Kwak would continue to have a market. According to the indictment, and in connection with their guilty pleas, the defendants admitted that Mr. Kwak owns and operates Viewtech, Inc., in Oceanside, California. Viewtech imports “free-to-air” or “FTA” satellite receiver boxes and sells them to the public through a network of retailers under the brand name “Viewsat.” According to the indictment, there is a limited amount of free programming available by

satellite to owners of FTA receiver boxes, much of it consisting of ethnic and religious programming in numerous languages. Yet, millions of Viewsat FTA boxes have been sold to the public. The popularity of FTA boxes is due to the fact that they are designed to make it a simple process for a purchaser to obtain subscription-based satellite television, such as that offered by Echostar's DISH Network, for free. DISH Network licenses copyrighted works from the copyright holders, encrypts the signal, and sells the right to view to DISH subscribers. Subscribers to DISH Network programming obtain from DISH a "smart card," which is inserted into a DISH satellite receiver box. The smart card decrypts the programming that the subscriber is authorized to view. Over the years, DISH has changed its encryption algorithms and employed other countermeasures to attempt to defeat theft of its signal. To illegally decrypt the DISH signal, the FTA boxes must appear to have DISH smart cards. That is done by reverse-engineering DISH smart cards and creating computer code which, when downloaded to an appropriate FTA box, will emulate the existence of a smart card and trick the system. In the past, as DISH encryption and countermeasures were defeated, the code has been posted on the Internet and made available for download to anyone.

In the late fall of 2007, DISH announced that it had created a new encryption scheme and would start shipping new smart cards to its customers. As the new encryption scheme was deployed, owners of FTA boxes would no longer be able to view DISH programming without a subscription, and sellers of FTA boxes would lose their market.

The defendants admitted in their plea that Mr. Kwak authorized Messrs. Allison and Ward to locate persons to work on cracking Nagra 3. Mr. Kwak agreed to provide funding and a substantial reward for success. Messrs. Allison and Ward admitted that they solicited a third party to join the scheme. Mr. Allison admitted purchasing a specialized microscope to be used in dissecting and analyzing smart cards for the third party and was reimbursed by Mr. Kwak. Mr. Kwak admitted meeting with and paying \$20,000 in cash to

the third party for photographs of a dissected smart card purported to be a Nagra 3 card. Mr. Kwak also admitted that he offered a reward of \$250,000 if the EPROM (eraseable programmable read-only memory) for the Nagra 3 card could be obtained.

The defendants tendered their guilty pleas before United States Magistrate Judge Anthony J. Battaglia, subject to final acceptance of the pleas by United States District Judge Janis L. Sammartino on January 22, 2010, at 9:00 a.m.

This case was investigated by Special Agents of the Cybersquad of Federal Bureau of Investigation in San Diego.

DEFENDANTS

Case Number: 09cr2646 -JLS

Jung Kwak
Phillip Allison
Robert Ward

SUMMARY OF CHARGE

One Count - Title 18, United States Code, Section 371: Conspiracy to Violate the Digital Millenium Copyright Act

Maximum Penalty: 5 years' imprisonment and \$250,000 fine

AGENCY

Federal Bureau of Investigation