

AFFIDAVIT

I, Tracy Marquis Kierce, being duly sworn hereby depose and say as follows:

1. I am employed as a Special Agent (SA) of the Federal Bureau of Investigation (FBI) and have been so employed since February, 1987. Since June, 2001, I have been assigned to investigate computer technology and intellectual property crimes. I have previously investigated a variety of white collar crime allegations including fraud against the government, bank fraud, advance fee schemes and telemarketing fraud. I have received training from the FBI regarding computer technology and intellectual property crimes.

2. I make this affidavit in support of a search warrant to search the premises located at 7309 Franklin Avenue, Apartment 204, Los Angeles, California, 90046, more thoroughly described in Paragraph 4 below (the "Subject Premises"), for evidence of violations of Title 18, United States Code, Section 1832 (Theft of Trade Secrets). I also make this affidavit in support of a criminal complaint and arrest warrant charging Igor Serebryany with violating Title 18, United States Code, Section 1832 (Theft of Trade Secrets). For the reasons set forth below, there is probable cause to believe that Igor Serebryany has knowingly stolen, and has without authorization appropriated, taken, and carried away, the trade secrets of DirecTV and NDS Americas,

Inc., with the intent to convert those trade secret to the economic benefit of someone other than the owner, knowing that the offense would injure the owner, and that evidence of this offense will be found at the Subject Premises.

3. The facts set forth below are based upon my own personal observations, upon reports and information provided to me by other law enforcement officers, and upon information provided to me by other individuals employed by or on behalf of DirecTV, including Larry Rissler, Vice-President of Signal Integrity at DirecTV, Megan McNulty, Vice President of Legal Affairs at DirecTV, individuals employed by or on behalf of NDS Americas, Inc. (NDS), including Richard L. Stone of Hogan & Hartson L.L.P., individuals employed by the Internet Crimes Group, Inc. (ICG), including Joshua I. Halpern, Director of Threat Management Services for ICG, and Joseph Farino, Senior consultant for ICG, and attorneys and other personnel from Jones, Day, Reavis and Pogue (Jones Day), including Rick McKnight, Regional Managing Partner at Jones Day, Kevin MacBride, Gregory Schetina, and David Boyce, partners at Jones Day, and other individuals. I have not included in this affidavit all information known by me relating to this investigation. Rather, I have set forth only those facts necessary to establish probable cause for the requested search warrant for the Subject Premises, the requested complaint and the requested arrest warrant charging

Igor Serebryany with violations of Title 18, United States Code, Section 1832.

THE SUBJECT PREMISES

4. The Subject Premises is commonly described as 7309 Franklin Avenue, Apartment 204, Los Angeles, California, 90046, and is more specifically described as apartment space located in a 5-story tan brick building trimmed with light green vertical designs. At the entrance to the building are double glass doors. A large gate to the West of the front entrance leads to the underground parking garage for the apartment building. The building is located at the Northwest corner of Franklin Avenue and Fuller Avenue. The letters "The Continental" and the numbers "7309" appear in green on the front of the building, which is located on the North side of the street. The hallways inside the building are painted light pink. Apartment 204 is located on the second floor of the building, and the numbers "204" are affixed to the apartment door, which is white.

TITLE 18, UNITED STATES CODE, SECTION 1832

5. Title 18, United States Code, Section 1832 (Theft of Trade Secrets) expressly provides as follows:

(a) Whoever, with intent to convert a trade secret, that is related to or included in a product that is produced for or placed in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly--

(1) steals, or without authorization appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information;

(2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information;

. . . .

shall . . . be fined under this title or imprisoned not more than 10 years, or both.

DESCRIPTION OF DIRECTV SATELLITE SIGNAL PROGRAMMING

6. DirectTV, a California corporation, delivers digital entertainment and television programming to millions of homes and businesses throughout the United States. A consumer wishing to subscribe to DirectTV television programming must first obtain necessary hardware items to receive the satellite signals. The necessary hardware includes a satellite dish, an integrated receiver/decoder ("IRD"), and an access card or "smart card." The access card, or smart card, operates the IRD. Satellite programming currently includes major cable networks, major studio movies, special event programming offered on a pay-per-view basis, local channels, and a variety of other sports and special interest programs and packages.

7. NDS is a developer and supplier of proprietary encryption and smart card technology to DirectTV, and DirectTV has distributed smart cards supplied by NDS throughout the United States. The access card or smart card enables or authorizes the

IRD to decrypt the encrypted transmissions from DirecTV satellites. The satellites, which are in geosynchronous orbit above the earth, relay encrypted signals to subscribers equipped with a dish and an IRD. The satellite signal is received by the dish and transmitted by wire to the IRD. The IRD contains a slot into which the access card is inserted, and the IRD processes the incoming signals.

8. An access card is provided to consumers along with the IRD. After a subscriber installs the dish and IRD at his or her home or business, and purchases one or more programming packages, the subscriber's access rights are electronically programmed on the access card by sending a signal through the satellite data stream to the subscriber's access card in the IRD. The access card contains computer chips with copyrighted software and acts as a re-programmable microprocessor using smart card technology to control the programming the subscriber can view based on the programming packages and programming purchased by the subscriber.

9. The access card is a key component in the security and integrity of the DirecTV satellite programming system. To prevent unauthorized signal reception and program viewing, transmissions of television programming are encrypted at uplink facilities. The access card enables the subscriber's IRD to decrypt the signals and permit program viewing in accordance with

the subscriber's authorized subscription package or pay-per-view purchases.

10. DirecTV has spent significant resources to protect the integrity of its satellite signals so that only authorized users are able to decrypt the programming. DirecTV combats theft by several means. One method employs electronic countermeasures (ECMs) that deny programming to illegally modified access cards. ECMs are electronic messages sent through the satellite data stream to deactivate illegally modified access cards. Some of the ECMs "loop" the unauthorized software in the access cards to make the access cards inoperable. A community of unauthorized computer programmers and hardware manufacturers, which is sometimes referred to as the "pirate community," is engaged in writing and distributing software on the Internet to circumvent these ECMs and develop hardware and software techniques to allow unauthorized users to obtain free satellite programming from DirecTV.

11. The pirate community is also actively engaged in manufacturing, distributing and selling unauthorized hardware devices that enable the unauthorized decryption of satellite signals. Such devices have limited or no legitimate commercial purpose other than to permit the illegal and unauthorized reception and decryption of encrypted television programming. One frequently used device that enables satellite signal theft is

referred to as an "unlooper," and can restore the illegally modified software in a looped access cards to allow the card to intercept and decrypt satellite signals without authorization. The "unlooper" and other hardware devices, including "card loaders," "programmer/readers," "AVRs," "blockers," "emulators" and "computers," are all used to facilitate the unauthorized interception of satellite television signals. These hardware devices are sometimes advertised on Internet web sites, in local publications, and in underground satellite publications.

12. To address the problem of unauthorized signal theft, in 1997 DirecTV introduced new access cards developed by its security vendor NDS to replace the original "first generation" access cards. New, supposedly secure second-generation cards, which are sometimes referred to as "Period 2" cards or "H" cards, were sent to all subscribers in 1997 to replace the first generation access cards. The pirate community developed ways to circumvent the H card by August 1997. The H Card is no longer manufactured and since August 2002 is no longer supported by DirecTV. In February 1999, DirecTV introduced a third generation access card, sometimes referred to as a "Period 3" card or an "HU" card. The first hack of the HU card was announced in November 2000 when a number of pirate Internet web sites advertised that they were selling illegally modified HU cards.

Today, HU cards can be illegally programmed to intercept DirecTV's programming services.

13. In August 2002, DirecTV began distributing a fourth generation access card, known as the "P4" card or the "Period 4" card. The Period 4 card was the result of two years of development efforts by DirecTV and NDS and contains sophisticated proprietary technology of DirecTV never before used in any smart card application. DirecTV has invested more than \$25 Million to develop the Period 4 access card. I have spoken to representatives from DirecTV who have confirmed to me that there are presently no known compromises of the Period 4 security features; the Period 4 access card is presently secure, although numerous Internet websites (most of which are hosted outside the United States) post information and techniques to support those attempting to develop ways to circumvent the security features of the Period 4 card.

14. Currently, there are several hundred web sites devoted to selling pirate hardware and software. The pirate hardware and software is used to modify Period 3 and previously Period 2 DirecTV access cards to unlawfully receive programming services without authorization ("pirate community websites"). DirecTV has recently replaced the Period 2 access cards with Period 4 access cards, but the Period 3 access card is used by the majority of DirecTV customers to receive DirecTV programming.

PROBABLE CAUSE THAT SEREBRYANY KNOWINGLY STOLE TRADE SECRETS:

15. On October 10, 2002, Assistant United States Attorney James W. Spertus, FBI SA Christopher Beausang and I responded to the Los Angeles office of Jones, Day, Reavis and Pogue, a law firm ("Jones Day"), to receive a criminal referral regarding the theft and publication of highly sensitive trade secret information owned by DirecTV and/or NDS. The trade secret information pertained to the development and design of the Period 4 access card, as well as information about the Period 3 card. Present at this meeting was Larry Rissler, Vice-President of Signal Integrity at DirecTV, Joshua I. Halpern, Director Threat Management Services for the Internet Crimes Group, Inc. (ICG), Joseph Farino, Senior consultant for ICG, and attorneys and other personnel from Jones Day, including Rick McKnight, Regional Managing Partner at Jones Day, and Kevin MacBride, Gregory Schetina, and David Boyce, partners at Jones Day. At this initial meeting, I learned the following:

a. Jones Day was outside counsel for DirecTV and represented DirecTV in civil litigation commenced on September 6, 2002 by DirecTV against NDS (the developer and supplier of the proprietary encryption and smart card technology for DirecTV as discussed above).

b. NDS had supplied all of DirecTV's smart cards, including the Period 4 access card that had begun to be

distributed to customers in or about April 2002. The Period 4 access card is presently the only DirecTV access card that has not been compromised by the pirate community.

c. The civil litigation filed by DirecTV against NDS includes breach of contract allegations and other related claims. The civil complaint and all related pleadings have been filed under seal in federal court to ensure that the pirate community does not gain access to trade secret information relevant to the allegations in the civil complaint.

d. In September 2002, DirecTV, through Jones Day, filed motions for expedited discovery in the civil litigation. Anticipating expedited discovery, DirecTV and Jones Day had, since August 2002, been actively reviewing documents both to prepare for document production in the civil litigation to comply with DirecTV's discovery obligations, and to use internally by Jones Day attorneys to prepare for the civil litigation.

e. As part of this effort to prepare for litigation, in August 2002 DirecTV delivered approximately 27 boxes of documents containing confidential material and trade secret information to Jones Day (the Incident Documents). Some of the information in the Incident Documents was so secret and valuable to DirecTV that DirecTV had previously maintained

the information only in encrypted format on computer hard drives secured at DirecTV facilities. Hard copies of such information was printed for the sole purpose of providing the information to Jones Day, as required by the civil litigation.

f. From August 2002 through October 2002, the Incident Documents were reviewed by Jones Day attorneys in the Jones Day Los Angeles offices in connection with the civil litigation.

g. In October 2002 and earlier, highly sensitive trade secret information pertaining to the development of the Period 4 access card was posted on pirate websites on the Internet (the Published Trade Secrets). The Published Trade Secrets concerned the development of the Period 4 access card and included highly confidential internal design notes and correspondence between DirecTV and NDS regarding the Period 4 access card architecture and security features.

h. To assist in the DirecTV civil litigation and other litigation matters for which Jones Day was counsel, Jones Day had retained a document imaging and management company named Uniscribe Professional Services (Uniscribe).

i. In August 2002 through October 2002, and earlier, Uniscribe operated an imaging center on the premises of Jones Day's Los Angeles office. The imaging center was

located in a fully enclosed room with a single operational entrance located inside the Jones Day office space of the Jones Day Los Angeles office. To access the imaging center, an individual must first pass through building security and use an access card programmed for elevator access to the floor on which the imaging center was located. After accessing this secured floor, the individual would then need a key to unlock the locked door of the imaging center.

j. The imaging center contained six computers dedicated for use by Uniscribe employees for the scanning, optical character recognition, and related document management services performed by Uniscribe for Jones Day. In addition, a separate computer located in the imaging center permitted communication with Jones Day personnel and access to the Internet.

k. When the Incident Documents were received by Jones Day from DirecTV, they were stored in rooms at Jones Day with controlled access, which access was limited to legal assistants and attorneys with cause to access the documents in connection with the DirecTV civil litigation. Jones Day attorneys and legal assistants were, at the time, compiling lists of critical documents that required immediate copying and segregation into binders. As a part of this process, some boxes of documents were flagged by Jones Day and sent

to the imaging center located inside the Jones Day law firm for reproduction. Following copying, boxes of documents were returned to the DirecTV case room.

l. In August and September 2002, the Incident Documents were provided by Jones Day to Uniscribe for imaging at the Jones Day imaging site on the Jones Day office premises. The Incident Documents were to be kept in a locked room and not leave the Jones Day premises, which is why Jones Day had arranged for onsite imaging.

m. The Uniscribe employees authorized to access the Jones Day premises to assist Jones Day with its document management needs during the months of August and September, 2002, were Yelena Tsvetkova, Peker L. Mikhaie (aka Michael Peker) and Abraham Filoteo. Each was required by Jones Day to read and adhere to Jones Day's written policy concerning confidentiality of client information, and each agreed to do so.

n. On September 13, 2002, Jones Day instructed Uniscribe to implement longer working hours to accelerate the necessary imaging of the Incident Documents. At this time, approximately 22 of the 27 boxes of Incident Documents were relocated to the imaging center. Without Jones Day's authorization, another individual, Igor Serebryany, then began helping to process the Incident Documents.

o. As part of the standard Uniscribe imaging process, Uniscribe would first scan a document intended for imaging. The scanned document resulted in a ".tif" format digital image of the document. Following scanning, Uniscribe employees would then append numbering codes and confidentiality statements to the .tif images, perform an OCR (Optical Character Recognition) scan of the imaged files, and create additional, related text files that contained the OCR version of the documents with the appended confidentiality statements. In a typical process, the OCR data and the final ".tif" images would be written to CDs that were either temporarily stored in the imaging center or provided to Jones Day attorneys. Additionally, a new hard copy, referred to as a "blowback," would be created and either temporarily stored in the imaging center or provided to Jones Day attorneys. Finally, the imaged documents would be digitally archived and housed on peripheral storage devices attached to systems in the imaging center.

p. On September 21, 2002, forum members on a pirate community website called PiratesDen.com, which is a website dedicated to discussions about circumventing DirecTV encryption technology, indicated publicly that they had access to highly sensitive, internal DirecTV and NDS

documents pertaining to the Period 4 access card (the Published Trade Secrets).

q. On September 23, 2002, attorneys for NDS informed counsel for DirecTV that confidential information relating to NDS technology and its business had been posted on the Pirates Den Discussion Forum and the Legal Rights Satellite Organization, both of which are websites dedicated to the topic of circumventing conditional access technologies protecting satellite signal programming. NDS claimed that it had strong reason to believe that the source of the information was from inside the DirecTV organization.

r. On October 7, 2002, upon first understanding that the Published Trade Secrets could have come from inside the Uniscribe imaging facility inside the Jones Day office space, Jones Day halted all imaging of the Incident Documents. At this time, Jones Day resumed possession of all DirecTV related documents still located in the imaging center, including all blowbacks that had been generated. Jones Day also resumed possession of two sets of five CD's containing the ".tif" files of the Incident Documents that had been created as part of the imaging process.

s. On October 8, 2002, Jones Day retained computer forensic specialists Joshua I. Halpern, Director of Threat Management Services for IGC, and Joseph Farino, Senior

consultant for ICG, to conduct a preliminary investigation to determine if the Published Trade Secrets were leaked from the Jones Day document imaging facility. Joshua Halpern's preliminary investigation confirmed that there was evidence that such a leak occurred from the Jones Day imaging facility, and Jones Day and DirecTV referred the matter to the FBI for a criminal investigation.

16. I have learned from ICG that Joshua I. Halpern is a qualified forensic examiner with the following training and experience:

a. Halpern is Director of Threat Management Services at ICG, Inc. Since joining ICG, Halpern has managed numerous incident response investigations and has led crisis management efforts in response to critical security incidents at Global 2500 corporations and leading eCommerce websites.

b. Prior to his promotion to Director of Threat Management, Halpern served as a Senior Associate and later a Project Manager in ICG's eBusiness Assurance and Incident Response practices. Additionally, Halpern completed an audit of eFraud risk for a top-ten US financial institution's on-line account application systems.

c. Halpern has also published articles and monthly columns regarding cyber-crime. Halpern has also been

invited to present to ASIS International, Information Systems Audit and Control Association (ISACA) seminars on data integrity and on-line fraud, INFRAGARD, and numerous private seminars and lectures at corporations and intellectual property law practices. He is an expert on forensic data recovery. Halpern received his bachelor's degree from Princeton University.

17. On or about October 15, 2002, I reviewed a report prepared by Halpern and learned the following:

a. On October 8th, 2002, Halpern inspected the Uniscribe facility at Jones Day and determined that there were 6 scanning-related computers that were electronically networked to one another via a hub. These 6 computers were not networked in any physically visible manner to additional hosts or internal networks. In addition to the 6 computers utilized for scanning purposes, there was an additional computer inside the imaging center that was owned by Jones Day and appeared to be connected via CAT-5 cabling to the Jones Day network.

b. Jones Day informed Halpern that this Jones Day computer was used by Uniscribe employees to access Internet resources such as email, and that it had the same access to the Internet afforded other Jones Day computers on the Jones Day network, such as access to the world wide web.

Timestamp Analysis:

c. On October 9, 2002, Halpern obtained from DirecTV a digital copy of the Published Trade Secrets, which consisted of 13 ".PDF" files that had been downloaded from a pirate web site. (I know from my own investigation that an FBI confidential informant had come across 3 of these ".PDF" files on the Internet, and I independently provided these files to Larry Rissler during the criminal referral meeting on October 10, 2002 for analysis and identification. Through our work with confidential informants, SA Beausang and I were aware of the Published Trade Secrets before receiving the criminal referral from DirecTV and Jones Day, as discussed above).

d. On October 10, 2002, Larry Rissler provided Halpern with a copy of the 3 ".PDF" files that had been downloaded and passed to the FBI by the FBI's confidential informant.

e. All of these ".PDF" files contained timestamp information, including the dates on which the files were created and the software that was used to create the files. Both the files obtained by DirecTV and the files that were independently provided to Rissler by the FBI indicated that an application named "PDF-IT version 5.09" had been used to convert the files. Files can be converted from one format

to another by software such as PDF-IT. For example, PDF-IT can convert files from single ".tif" images to ".PDF" compilations of numerous, individual ".tif" images.

f. Two computers in the Uniscribe imaging facility had copies of PDF-IT version 5.09 software installed on them when ICG imaged the drives on October 8, 2002.

g. In addition to the above-describe file creation analysis, the time-stamp analysis similarly confirmed that the files obtained by DirecTV and the files obtained by the FBI were copies of the same files created during the imaging of the Incident Documents in the Jones Day document imaging facility. All of the files were created on either September 17, 2002, or September 19, 2002. (I know from my independent investigation that these dates are consistent with the time period during which "Maxximus," who was the website administrator for the website DSSHackers.com, received the Published Trade Secrets from "Igor32" as set forth below.)

Comparison of Incident Documents and Uniscribe Tif's:

h. Halpern also compared copies of the ".tif" images, which are the immediate output of the Uniscribe scanning processes described above, with copies of the same images contained in the PDF files of the Published Trade Secrets obtained from the Internet by DirecTV and provided to

DirectTV by the FBI. Halpern determined that there were numerous examples of identical content in the compared data sets.

i. Many of the .tif files and .PDF files were created from the same scanning process; the distortion caused by scanning or faxing the original documents was identical between both data sets for each comparison made by Halpern.

j. In order for these similarities to be present, the Published Trade Secrets must have originated from digital copies of scans made by Uniscribe - not hard copies made from Uniscribe scans. A rescanning process would have added additional graphical distortion to at least some of the documents, and Halpern noted no instances of differences in distortion between the compared data sets.

Internet Access to Hacking Sites from the Imaging Center

k. As described above, one of the computers located inside the Jones Day imaging center was connected to the Internet, although not connected in any physical manner to the computers that were used to image the Incident Documents. On this Internet-connected computer, the operating system's Internet history included undated, non-user specific entries for the websites DSS-Hackers.com, DSSArmy.com, and DSSRookie.com.

1. Additionally, Halpern performed a keyword search across all data contained on the hard disk drive of the Internet connected computer and located traces of a Google.com Internet search performed by an unknown user of the machine on September 16, 2002, at 6:45 P.M. Google is an Internet search engine that can be used to locate websites by keyword searches. This September 16, 2002 Google search was for the string of characters "vcipher," and the results page included numerous references to the pirate website Vcipher.com. Halpern also recognized that the files of the Published Trade Secrets he had analyzed as discussed above included numerous references to Vcipher.com.

Halpern's Conclusion

m. Halpern is confident that the Published Trade Secrets were originally obtained as digital copies of ".tif" images produced during the standard Uniscribe imaging process at the imaging facility located inside the Jones Day Los Angeles office space.

INTERVIEW OF MAXXIMUS

18. After receiving the criminal referral on October 10, 2002 as discussed above, I determined through various sources that the Published Trade Secrets were first published to the website administrator of the website DSS-Hackers.com. I then identified the true name identity of this website administrator,

and determined that he uses the online screen name MAXXIMUS. I then briefed other FBI SAs with some of the facts set forth above regarding this investigation, and requested that these FBI SAs interview MAXXIMUS. I subsequently read a report of this interview, and learned the following:

a. MAXXIMUS acknowledged that he was the administrator of the website DSS-Hackers.com. Sometime back in September 2002, he received an e-mail from an individual who identified himself as "Igor." Igor claimed to have internal documents belonging to DirecTV and NDS and indicated that he would have access to the documents for a very limited time. Igor wanted to get these documents posted on the Internet.

b. Igor told MAXXIMUS that he (Igor) had located DSS-Hackers.com through a Google search. MAXXIMUS did not know Igor and had not had any previous contact with him. MAXXIMUS did not know if Igor was a disgruntled employee of DirecTV or NDS, a hacker, or some other insider.

c. Igor told MAXXIMUS that he had to convert all of the documents into Adobe format before sending them. (I know from my training and experience that documents in Adobe format bear the "PDF" extension.) Igor wanted to get all the documents posted on the internet.

d. Igor sent MAXXIMUS some documents through Yahoo Messenger. MAXXIMUS also sent some of the document he received to a website called the PiratesDen.com. MAXXIMUS did not pay Igor for the documents, and did not receive any compensation for sending the documents to the PiratesDen website.

e. Igor had too many documents for MAXXIMUS to upload to his server. The hosting company for MAXXIMUS' website is located in Hong Kong, and MAXXIMUS did not upload any documents from Igor to his server.

f. There is a moderator on MAXXIMUS's website who had a friend in Canada who had a server that would allow Igor to upload the documents by file transfer protocol (FTP), which is a method that enables the transfer of large files. (I know from my training and experience that large files cannot readily be e-mailed as attachments through e-mail hosts such as Yahoo because the Internet Service Providers such as Yahoo will reject large file transfers.) Igor transmitted the documents by FTP to this server.

g. MAXXIMUS has not had any other contact with Igor. MAXXIMUS did not pay Igor for the documents and was not paid to forward the documents to anyone else. MAXXIMUS got rid of the documents and all records pertaining to his dealings with Igor upon realizing the confidential and proprietary

information in the documents could create a problem for him from a legal standpoint. MAXXIMUS has had no further contact with Igor.

PHYSICAL EVIDENCE FOUND IN THE JONES DAY IMAGING CENTER

19. At the October 10, 2002, criminal referral meeting described above, Jones Day attorneys informed me that they were planning to immediately change the locks on the door of the Jones Day imaging center to prevent all access to the room as part of its internal investigation of how the Published Trade Secrets were stolen.

20. On November 15, 2002, I traveled to the Jones Day imaging center to observe the facility and I observed the following items:

a. A handwritten work schedule for Igor that indicated that Igor worked in the imaging center from September 1-6, 2002.

b. Another hand written work schedule for Igor that indicated that Igor worked in the imaging center September 16-20, 2002, and September 22-28, 2002.

c. A CD mailer from Smart-eStore Processing Center addressed to Igor Serebryany, 7309 Franklin Avenue #204, Los Angeles, CA. 90046 (the Subject Premises).

21. At my request, I was allowed to take the above-described items, and other items, into evidence, and I left a receipt for these items at Jones Day.

22. In addition, on November 15, 2002, I was provided a printout of a surveillance photograph from the Jones Day building security camera of Mikhaie and Igor entering the elevators in the Jones Day building on September 22, 2202 at 10:39 a.m.

INTERVIEW OF IGOR SEREBRYANY

23. On December 17, 2002, SA Beausang and I interviewed Igor Serebryany at the FBI Los Angeles Field Office. Serebryany was advised of the identities of the interviewing agents and the purpose of the interview, and provided the following information:

a. Serebryany's uncle, Michael Peker, is employed by Uniscribe Corporation.

b. Pecker worked this past Summer scanning documents at the law firm Jones, Day, Reavis & Pogue in Los Angeles, California.

c. Due to the large work load, Peker asked Serebryany to assist him, and Serebryany agreed. Serebryany worked with his uncle at Jones Day for approximately one week at the beginning of September 2002. Serebryany then took one week off before working at Jones Day for approximately one and one-half more weeks.

d. Peker used an access badge to get himself and Serebryany into the Jones Day building, and Peker paid Serebryany for his assistance.

e. Serebryany and Peker worked a shift at Jones Day from Monday to Friday that began at approximately 4:00 p.m. and continued until approximately 11:00 p.m. On the weekends, Serebryany and Peker worked a day shift.

f. The Uniscribe supervisor at the Jones Day site was Abraham Filoteo, who also worked with Serebryany and Peker. Another Uniscribe employee named Yelena sometimes worked with Serebryany and Peker.

g. During the second one and one-half weeks that Serebryany worked at the Jones Day facility, Serebryany scanned documents pertaining to DirecTV. There were a total of between 38 and 40 boxes of DirecTV documents. Serebryany also worked on scanning documents pertaining to a another case involving another Jones Day client.

h. Serebryany had limited knowledge of DirecTV until he began to work on scanning the DirecTV documents at the Jones Day site.

i. Most of the documents pertained to the history and development of DirecTV's P4 access card. Serebryany further remembered that there may also have been some documents containing technical specifications for the card.

j. Serebryany knew that NDS was an Israeli company, but did not know anything more about NDS and did not know anyone at the company.

k. Serebryany created two compact disks (CDs) which consisted of DirecTV documents that had been scanned as ".tif" files. Peker was out of the office when Serebryany created these CDs.

l. Serebryany also performed a search for DSS hacking websites using the Google search engine, and the first result listed from his search was for a site named DSSHackers.com. This initial search was performed from a computer connected to the Internet located in the Jones Day Imaging Center. This computer was located in the far corner of the imaging center, on the right-hand side of the room upon entry into the room.

m. Serebryany converted the .tif files on the above-referenced CDs to .PDF files on his father's computer at his parents' residence (the Subject Premises).

n. In the first of two sessions during which Serebryany attempted to provide the documents he obtained from Jones Day to the hacking community, Serebryany sent more than 10 megabytes of the documents to the administrator of DSSHackers.com, who went by the online nickname Maxximus.

o. Serebryany used his father's computer (located at the Subject Premises) to send these documents to an FTP site address that had been provided to him by Maxximus.

p. On the second day, Serebryany sent a second set of DirectTV documents from the same computer (located at the Subject Premises). He sent a total of approximately 800 megabytes to Maxximus.

q. Serebryany's father's computer (located at the Subject Premises) was connected to the Internet through a DSL account subscribed to through Pacific Bell. The account is in the name of Serebryany's mother, Irena Serebryany. Serebryany's father's name is Alex Serebryany.

r. Maxximus later told Serebryany via e-mail that the documents he had sent were too sensitive to be posted in DSSHackers.com.

s. Serebryany was upset by this and considered sending e-mails to other visitors to the forum that would inform them that Maxximus had the information but was not sharing it with them.

t. Maxximus later sent to Serebryany an e-mail which asked if Serebryany had posted the above-referenced files on any other sites. The interviewing agents asked Serebryany this same question, and Serebryany said that he had not.

u. Serebryany had never before been in control of sensitive and confidential information like that in the DirectTV documents. He was not directed or paid by anyone to send the above-referenced documents to Maxximus. Serebryany sent the files to Maxximus because the files were confidential, and because it was in his power to do so. Serebryany specifically stated that he wanted to help the DSS hacking community. Serebryany was adamant about having sent the documents to Maxximus solely for these reasons.

v. Serebryany claimed to have had no prior contact with the satellite television pirate community. In addition, he had not previously visited DSSHackers.com or any other forum devoted to satellite signal piracy.

w. Some of the above-referenced files had remained on Serebryany's father's computer (located at the Subject Premises). However, Serebryany subsequently re-formatted the drive and it later crashed. Serebryany installed a new hard drive in the computer, but kept the original drive.

x. Serebryany no longer has the two CDs referenced above and does not know where they are.

y. I showed Serebryany a CD holder obtained from the imaging center at the Jones Day site, which bore the mailing address Igor Serebryany, 7309 Franklin, Suite 204, Los Angeles, CA 90046 (the Subject Premises). This CD holder

contained a CD labeled "The Doors LA Woman." Serebryany stated that he had brought the CD holder to Jones Day to protect the CDs that he made containing the DirecTV documents described above.

z. I showed Serebryany a Jones Day imaging center "Request for Imaging Services" for the DirecTV account with a yellow post-it containing the words "Highly Confidential" "Attorneys' Eyes Only" and "Privileged." Serebryany stated that he was familiar with this form, and that he had filled out one of these forms while working at the Jones Day imaging center.

aa. Serebryany acknowledged that the words "Highly Confidential" "Attorneys' Eyes Only" and "Privileged" were added to the DirecTV documents after they were scanned.

bb. I showed Serebryany handwritten and weekly time sheets containing dates and hours worked by "Igor," and Serebryany stated that the handwriting was that of Peker and further stated that the dates and hours appeared to be accurate for Serebryany's work schedule at Jones Day.

E-MAIL ACCOUNTS RELATED TO IGOR SEREBRYANY

24. My investigation has determined that the following E-mail addresses are related to Igor Serebryany:

- i. Igor32@pacbell.net;
- ii. Igor_32@yahoo.com;

iii. Igor47@uchicago.edu;

iv. Igor32@flashnet.com.

DIRECTV'S EFFORTS TO PROTECT THE SECRECY OF ITS TRADE SECRETS

25. I have reviewed information provided by DirecTV to the government on December 27, 2002, and have learned the following:

a. The Published Trade Secrets included documents and technical information concerning the design, architecture and technology used in DirecTV's Period 4 and Period 3 access cards. The information pertained to the smart card technology, which is among DirecTV's most sensitive and valuable technology.

b. DirecTV has adopted extraordinary measures to protect its trade secrets. The detailed security procedures used by DirecTV were developed by or derived from those of Hughes Electronics Corp., DirecTV's parent company and a long-time military contractor to the United States government.

c. For example, all DirecTV employees have written employment agreements, which include obligations that survive their term of employment, to protect the confidential information of DirecTV and third parties that provide services and products to DirecTV. Consultants and contractors who work for DirecTV are also required to sign confidentiality agreements with DirecTV and Industrial

Rights Property Agreements, each of which further safeguards the trade secrets and confidential information of DirecTV and third parties who provide their confidential information to DirecTV.

d. DirecTV also has ongoing employee training programs, overseen and in many circumstances conducted by DirecTV attorneys, which provide recurring on-site training to DirecTV employees about the need to protect trade secrets and confidential information and how such information is to be treated internally in order to secure its protection. Additional and specific instruction is provided to the engineering staff in general, and very specific guidance and training is provided to those working in the area of conditional access engineering.

e. In addition, all contracts between DirecTV and any third parties relating to relationships which might involve the disclosure of confidential information include carefully drafted confidentiality provisions governing the permitted use and required protection for the subject information. In cases involving highly sensitive information, such as conditional access information, the requirements are particularly restrictive and, in most or all cases, perpetual.

Physical Security

f. DirectTV maintains a controlled, "badged environment" in all facilities. All employees and visitors to DirectTV's offices and facilities are required to wear a badge at all times. Badges are different to reflect whether an individual is an employee, a contractor, or a visitor, and access to certain areas and information are accordingly restricted. All visitors to DirectTV's offices and facilities must sign in, show identification, disclose if they have a computer with them, and must be accompanied by a DirectTV employee at all times. Professional security agents maintain security checkpoints at the entrances of the facilities, and must confirm that every person entering has a valid badge. All bags are subject to search, both entering and exiting. Certain products, e.g. computers, are not allowed into or out of the facility without appropriate prior approval of an authorized executive of the company.

g. Certain areas of DirectTV's facilities are further restricted. In particular, the separate building that houses DirectTV's engineering staff has both security guard stations and specially restricted elevator access. Only those DirectTV employees who have been specifically approved, and their badges specifically authorized, can access the three DirectTV engineering floors in this building. In this

engineering facility, some employee badges are authorized for access only during business hours, Monday through Friday, while other badges have 24-hour access at all times. This badge authorization for this facility, in particular, a separate floor of this facility that houses the engineers working on Conditional Access Engineering (including smart cards), is reviewed on a monthly basis to confirm that only authorized personnel are being permitted to access the facility.

h. Within the separate floor of the Engineering Building, which houses in part the engineers working on Conditional Access technology including smart cards, a portion of the floor is further walled-off and access is further restricted. The doors to that section of the floor are locked by cipher locks, the combinations of which are changed frequently and known only to a limited group of identified DirecTV employees who work behind the wall and their supervisor, DirecTV's Vice President of Conditional Access Engineering. Access by others to that area requires that they ring a bell for admittance, sign a log book both upon entry and exit, and be escorted at all times by an employee of that unit while in the secured section.

i. Wall-mounted cameras record all entry and exit from this secure area 24 hours a day, 7 days a week. Exit

from the area requires the code to be used in the cipher lock to unlock the door from the inside. Exit cannot be made without inputting the code. Internal movement to certain rooms within this area is still further restricted by locked doors with locks requiring special authorization to enter or exit.

Document and Communications Security

j. DirecTV employs a number of measures to protect the security of documents and communications about conditional access engineering matters. For instance, as previously noted all third parties having access to any such information are subject to stringent contractual obligations limiting use and requiring the protection of all confidential information. In addition, DirecTV has developed and implemented special written policies and procedures that are strictly followed in order to maintain secrecy. Specifically, the P4 technology is not divulged, even within DirecTV, except on a "need to know" basis. Only a select few DirecTV engineers have access to the P4 technology.

k. Further, the development projects and third party contractors who work on those projects, such as silicon chip manufactures and consultants, are assigned code names and are referenced only by those code names in all communication

and correspondence, even within DirecTV. The name of the company who develops and manufactures the chip for the DirecTV smart cards is one such contractor whose name is guarded, and DirecTV security protocols require that the vendor's true name not be used unless in a secure communication (i.e., an e-mail encrypted with PGP encryption software).

l. DIRECTV requires that all communications about the P4 technology be sent via encrypted messages whether it is by e-mail or telephone, internal or external. As noted, in communications, each of the vendors who supply portions of the P4 technology to DirecTV is referred to by code name.

m. Whenever a writing references DirecTV's P4 technology, it must be printed on specific colored paper so it can be easily identified on sight, thereby decreasing possible theft of that writing. Work-related conditional access information, such as smart card materials, cannot remain on desks after hours. Such material must either be locked up or shredded. Discarded information is not collected with normal trash, but is destroyed separately.

n. In DirecTV's relationship with NDS, its security vendor, certain security protocols were observed. When DirecTV provided its P4 technology to NDS for incorporation into the P4 CAM, this highly sensitive technology was

transmitted using two separate encryption tools in order to prevent any possibility of interception and decryption. In addition, all phone and e-mail communications between DirecTV and the vendor who worked on the P4 CAM were encrypted. Certain other P4 technology was shared only with the chip manufacturer and not with NDS pursuant to the "need to know" protection.

o. In addition to the foregoing document security measures, engineers working in sensitive areas use phones outfitted with voice encryption hardware.

Electronic Security

p. In general the internal networks of DirecTV are subject to standard industry practices to assure security. Firewalls and other security measures are used by the IT department to maintain security of the internal networks of the company. Remote access to networks is controlled by token-based security devices and is permitted only to authorized employees.

q. In addition, the computer network within the conditional access area is independent of other DirecTV networks, and isolated to the secured area of the Engineering Building. No external connections of this network are permitted. Only specifically authorized personnel with a "need to know" have access to the

information stored on these systems. No wireless connections are permitted.

r. The highly sensitive information relating to the conditional access technology and operations generally exists only in electronic form, as encrypted files on secured computers. Hard copy is generally not produced or permitted. Passwords allowing access to these data records are strictly limited to the key personnel having a need to know.

Security at Jones Day for the Civil Litigation

s. Prior to DirecTV filing its complaint against NDS in September 2002, DirecTV required that its outside counsel, Jones Day Reavis & Pogue, have all attorneys who were to work on the DirecTV matter equip their computers with PGP encryption software, and all communications (both internally at Jones Day and externally with DirecTV) were required to be encrypted for security.

t. DirecTV instructed Jones Day to file the complaint and subsequent pleadings under seal to insure the secrecy of P4 information discussed in the complaint, in particular, the names of third party subcontractors who worked on the P4 access card and certain technology that was incorporated into the P4 access card.

u. When DirecTV collected documents that would be required by law to be disclosed in the lawsuit as part of discovery, many of the more sensitive documents had never existed in hard copy form, but had only existed in soft copy encrypted on the hard drives of one or two DirecTV engineers. DirecTV printed only one copy of such documents in order to maintain their secrecy, and that single copy was sent to Jones Day so that DirecTV would be prepared to comply with discovery should the Court grant early discovery.

v. Jones Day was instructed to maintain the documents in a locked room, access to which was limited to only the attorneys and support personnel under their supervision working on the DirecTV matter. Jones Day was instructed that the documents were to be copied internally at Jones Day and not sent out to an outside copy center. Although use of an outside copy facility is standard and significantly less expensive, DirecTV elected to pay the additional cost in order to better maintain the physical security of these documents dealing with DirecTV's trade secrets, such as the design, architecture, and manufacture of the P4 smart card.

w. Further, Jones Day on behalf of DirecTV retained one of DirecTV's security contractors, Internet Crimes Group, to provide advice on security during the litigation,

including to further insure the secrecy and security of the DirecTV documents. Jeff Bedser of Internet Crimes Group met with Jones Day attorneys representing DirecTV in early September and discussed and advised Jones Day concerning network security.

x. After the theft of the Published Trade Secrets became known, DirecTV retrieved all documents, both hard copy and electronic forms, from Jones Day's offices and stored them in locked drawers and safes in the secure section of the DirecTV engineering facility. The documents have not left that secure area since being returned by Jones Day.

26. On October 16, 2002, FBI personnel acting at my direction requested the current address from the California Department of Motor Vehicles (DMV) for Igor Serebryany and determined that Serebryany's current DMV address was 7309 Franklin Avenue, Apartment 204, Los Angeles, CA 90046 (the Subject Premises).

27. I know from my investigation that Igor Serebryany is a student at the University of Chicago, located in Chicago, Illinois, but that he is presently residing at the Subject Premises. Serebryany intends to return to Chicago on January 5, 2003.

28. I know from my training and experience, and from speaking to individuals involved in the unlawful re-programing of DirectTV access cards, that the unlawful acquisition of useful code and other information about DirectTV access cards is very difficult to obtain and often requires the investment of a great deal of time and effort. Individuals who unlawfully gain access to such information are therefore likely to keep the information for extended periods of time. In addition, based on the fact that much of the evidence in this trade secret theft investigation will be forensically recovered computers and computer storage media, I believe that evidence will likely be kept on the computers used by Serebryany for years, including the computer owned by Serebryany's father located at the Subject Premises that Serebryany admitted he used to transmit the documents he took from Jones Day.

29. Based upon the facts set forth above, and upon my training and experience, I believe there is probable cause to believe that the Subject Premises is the residence for Igor Serebryany, and that evidence of Serebryany's theft of trade secrets as described above will be located at the Subject Premises.

COMPUTER DATA:

30. Based upon my training, experience and information related to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices including hard disk drives, floppy disks, compact disks, magnetic tapes and memory chips. I also know that during the search of the premises it is not always possible to search computer equipment and storage devices for data for a number of reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all of the necessary technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software application or operating system that is being searched.

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover "hidden," erased, compressed, encrypted or password-

protected data. Computer hardware and storage devices may contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises. A single megabyte of storage space is the equivalent of 500 double-spaced pages of text. A single gigabyte of storage space, or 1,000 megabytes, is the equivalent of 500,000 double-spaced pages of text. Storage devices capable of storing fifteen gigabytes of data are now commonplace in desktop computers. Consequently, each non-networked, desktop computer found during a search can easily contain the equivalent of 7.5 million pages of data, which, if printed out, would completely fill a 10' x 12' x 10' room to the ceiling.

d. Computer users can attempt to conceal data within computer equipment and storage devices through a number of methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension ".jpg" often are image files; however, a user can easily change the extension to ".txt" to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a "dongle" or "keycard," is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called "steganography." For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is evidence, contraband or instrumentalities of a crime.

ITEMS TO BE SEIZED:

31. Based on the foregoing, I respectfully submit that there is probable cause to believe that the following items, which constitute evidence of violations of 18 U.S.C. 1832 will be found at the Subject Premises:

a. Records, documents, programs, applications and materials relating to information obtained from the law firm Jones, Day Reavis and Pogue;

b. Records, documents, programs, applications and materials relating to the DirecTV Period 4 access card;

c. Records, documents, programs, applications and materials relating to purchasing, selling, manufacturing and/or distributing hardware devices or software primarily of assistance in the unauthorized decryption of direct-to-home satellite services;

d. Records, documents, programs, applications and materials relating to modified DirecTV access cards;

e. Records, documents, programs, applications and materials relating to the following E-mail addresses:

i. Igor32@pacbell.net;

ii. Igor_32@yahoo.com;

iii. Igor47@uchicago.edu;

iv. Igor32@flashnet.com;

f. Correspondence, memoranda and other records pertaining to the law firm Jones, Day, Reavis and Pogue, or Uniscribe Professional Services;

g. Opened and unopened e-mails and other correspondence that evidences the transfer of information obtained from Jones, Day, Reavis and Pogue, DirecTV, or is

related in any manner to the development of DirecTV access cards or is of assistance in the unauthorized decryption of direct-to-home satellite services;

h. Indicia of occupancy, including: invoices, letters, bills, personal effects, and mortgage and loan agreements tending to show ownership, occupancy, or control of the premises or the above described items;

i. Diaries, appointment books, calendars, day planners, address and telephone books that reflect scheduled meetings and dates;

j. Programs, materials or proprietary information belonging to DirecTV, NDS or Jones Day Reavis & Pogue;

k. As used above, the terms records, documents, programs, applications, materials, correspondence, memoranda, e-mails, indicia of occupancy, and proprietary information includes such items that can be modified or stored in any form.

l. In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

i. Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial

review of any computer equipment and storage devices to determine whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.

ii. If the computer personnel determine it is not practical to perform an on-site search of the data within a reasonable amount of time, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

iii. In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

iv. If the computer personnel determine that the data does not fall within any of the items to be seized pursuant to this warrant or is not otherwise legally seized, the government will return these items within a reasonable period of time not to exceed 60 days from the date of seizure unless further authorization is obtained from the Court.

m. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

i. Any computer equipment and storage device capable of being used to commit, further or store evidence of the offense listed above;

ii. Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;

iii. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC

cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

iv. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software.

v. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

vi. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

vii. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

32. It may also be necessary for programmers and other outside experts to assist the FBI during the examination of the computer evidence in order to help identify the significance and ownership of the seized items and trace the programs, other property, or access codes improperly obtained from DirecTV, NDS, or Jones Day, Reavis & Pogue to their source. Likewise, it may be necessary for programmers and other outside experts to assist

the FBI in interpreting and analyzing any software programs, stored documents, or other properly seized items to determine whether the items pertained to the theft of trade secrets described elsewhere in this affidavit. Further, it may be necessary for outside experts and consultants to assist the FBI with the search of the Subject Premises to identify the specified items to be seized as described above that relate to the theft of trade secrets investigation described above, including items pertaining to the development of the Period 4 access card and other items pertaining to the programming, distributing, manufacturing or selling of devices primarily of assistance in the unauthorized decryption of direct-to-home satellite services.

I declare under penalty of perjury that the foregoing is true and correct.

Tracy Marquis Kierce
Special Agent
Federal Bureau of Investigation
Los Angeles, California

Sworn and subscribed to before
me this 31st day of December, 2002.

UNITED STATE MAGISTRATE JUDGE

ATTACHMENT A

THE SUBJECT PREMISES

The Subject Premises is commonly described as 7309 Franklin Avenue, Apartment 204, Los Angeles, California, 90046, and is more specifically described as apartment space located in a 5-story tan brick building trimmed with light green vertical designs. At the entrance to the building are double glass doors. A large gate to the West of the front entrance leads to the underground parking garage for the apartment building. The building is located at the Northwest corner of Franklin Avenue and Fuller Avenue. The letters "The Continental" and the numbers "7309" appear in green on the front of the building, which is located on the North side of the street. The hallways inside the building are painted light pink. Apartment 204 is located on the second floor of the building, and the numbers "204" are affixed to the apartment door, which is white.

ATTACHMENT B

ITEMS TO BE SEIZED

The following items, which constitute evidence of violations of 18 U.S.C. 1832, found at the Subject Premises:

1. Records, documents, programs, applications and materials relating to information obtained from the law firm Jones, Day Reavis and Pogue;
2. Records, documents, programs, applications and materials relating to the DirecTV Period 4 access card;
3. Records, documents, programs, applications and materials relating to purchasing, selling, manufacturing and/or distributing hardware devices or software primarily of assistance in the unauthorized decryption of direct-to-home satellite services;
4. Records, documents, programs, applications and materials relating to modified DirecTV access cards;
5. Records, documents, programs, applications and materials relating to the following E-mail addresses:
 - a. Igor32@pacbell.net;
 - b. Igor_32@yahoo.com;
 - c. Igor47@uchicago.edu;
 - d. Igor32@flashnet.com;
6. Correspondence, memoranda and other records pertaining to the law firm Jones, Day, Reavis and Pogue, or Uniscribe Professional Services;
7. Opened and unopened e-mails and other correspondence that evidences the transfer of information obtained from Jones, Day, Reavis and Pogue, DirecTV, or is related in any manner to the development of DirecTV access cards or is of assistance in the unauthorized decryption of direct-to-home satellite services;
8. Indicia of occupancy, including: invoices, letters, bills, personal effects, and mortgage and loan agreements tending to show ownership, occupancy, or control of the premises or the above described items;

9. Diaries, appointment books, calendars, day planners, address and telephone books that reflect scheduled meetings and dates;

10. Programs, materials or proprietary information belonging to DirecTV, NDS or Jones Day Reavis & Pogue;

11. As used above, the terms records, documents, programs, applications, materials, correspondence, memoranda, e-mails, indicia of occupancy, and proprietary information includes such items that can be modified or stored in any form.

12. In searching for data capable of being read, stored or interpreted by a computer, law enforcement personnel executing this search warrant will employ the following procedure:

a. Upon securing the premises, law enforcement personnel trained in searching and seizing computer data (the "computer personnel") will make an initial review of any computer equipment and storage devices to determine whether these items can be searched on-site in a reasonable amount of time and without jeopardizing the ability to preserve the data.

b. If the computer personnel determine it is not practical to perform an on-site search of the data within a reasonable amount of time, then the computer equipment and storage devices will be seized and transported to an appropriate law enforcement laboratory for review. The computer equipment and storage devices will be reviewed by appropriately trained personnel in order to extract and seize any data that falls within the list of items to be seized set forth herein.

c. In searching the data, the computer personnel may examine all of the data contained in the computer equipment and storage devices to view their precise contents and determine whether the data falls within the items to be seized as set forth herein. In addition, the computer personnel may search for and attempt to recover "deleted," "hidden" or encrypted data to determine whether the data falls within the list of items to be seized as set forth herein.

d. If the computer personnel determine that the data does not fall within any of the items to be seized pursuant to this warrant or is not otherwise legally seized, the government will return these items within a reasonable

period of time not to exceed 60 days from the date of seizure unless further authorization is obtained from the Court.

e. In order to search for data that is capable of being read or interpreted by a computer, law enforcement personnel will need to seize and search the following items, subject to the procedures set forth above:

f. Any computer equipment and storage device capable of being used to commit, further or store evidence of the offense listed above;

g. Any computer equipment used to facilitate the transmission, creation, display, encoding or storage of data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices, and optical scanners;

h. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, and personal digital assistants;

i. Any documentation, operating logs and reference manuals regarding the operation of the computer equipment, storage devices or software.

j. Any applications, utility programs, compilers, interpreters, and other software used to facilitate direct or indirect communication with the computer hardware, storage devices or data to be searched;

k. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the computer equipment, storage devices or data; and

l. Any passwords, password files, test keys, encryption codes or other information necessary to access the computer equipment, storage devices or data.

13. Programmers and other outside experts may assist the FBI during the examination of the computer evidence in order to help identify the significance and ownership of the seized items and trace the programs, other property, or access codes improperly obtained from DirectTV, NDS, or Jones Day, Reavis &

Pogue to their source. Likewise, programmers and other outside experts may assist the FBI in interpreting and analyzing any software programs, stored documents, or other properly seized items to determine whether the items pertained to the theft of trade secrets described elsewhere in this affidavit. Further, outside experts and consultants may assist the FBI with the search of the Subject Premises to identify the specified items to be seized as described above that relate to the theft of trade secrets investigation described above, including items pertaining to the development of the Period 4 access card and other items pertaining to the programming, distributing, manufacturing or selling of devices primarily of assistance in the unauthorized decryption of direct-to-home satellite services.