EXHIBIT 1

CERTIFICATION OF MICHAEL GRENNIER, CFCE, EnCE

I Michael Grennier, CFCE EnCE, of full age and duly sworn, does hereby state as follows:

1. On February 26th, 2011, I forwarded the certification per both parties request and according to the conference call of both parties held on February 25th, 2011. (See attached as Exhibit A).

2. Steward Kellar, Esq., Defense counsel representing Mr. George Hotz, agreed to the process listed in the attached certification, as long as the bit-stream image of the drive was wiped after the searching processes were completed. He would not agree. however to begin the process on Monday, February 28, 2011, where Mr. Hotz would provide unencrypted access to The Intelligence Group for purposes of creating an unencrypted bit-stream copy of his clients hard drives, believing that a motion would be filed in order for Plaintiff to maintain a preserved copy for discovery purposes. Mr. Hotz clearly stated that his client would never agree to ANY copy being created, which could be retained for purposes other than the impoundment order and the processes mentioned in my first certification.

3. After sending my requested certification to both parties, I was advised that Mr. Hotz will not agree to any bit-stream copies of the hard drives. It was further proposed by Defendants counsel that we use Mr. Hotz's computer and operating system to conduct the searches and securely delete the data.

4. According to the Cyber Security Institute, Computer Forensics is defined at the preservation, identification, extraction, interpretation, and documentation of computer evidence, to include the rules of evidence, legal processes, integrity of evidence, factual reporting of the information found, and providing expert opinion in a court of law or other legal and/or administrative proceeding as to what was found. In basic terms, Computer forensics is a science

in which fact based results of an examiners findings should achieve the same result of any other computer forensic examiner. The use of standards and controls in scientific experiments is a fundamental axiom of the scientific method. No experiment can be considered "scientific" unless they are used to ensure reliable results. An important consideration is the nature of the scientific experiment itself as it may require the use of multiple standards and controls. Likewise, this axiom holds true in forensic science. A scientific experiment is a controlled experiment. Variables are intentionally introduced or changed one at a time and the results monitored. Physical evidence is analyzed using methods and procedures that have previously been verified or validated with the use of appropriate standards and controls. Therefore, all forensic science disciplines must document in their methods and procedures specific standards and controls. They must be used when analyzing physical evidence as a means to demonstrate that scientific principles and quality assurance practices were followed. Their use will also ensure that the methods, procedures, and instrumentation are functioning correctly, and that the results obtained are accurate, reliable, and repeatable. [1] For these reasons, we maintain a computer forensics lab where I test our hardware and software to ensure that they are working properly and use only software and hardware which is known to me and my lab personnel. In order for TIG to isolate, segregate and/or remove the information on those devices related to Defendant's circumvention devices, I recommend these standard principles to be applied.

5. Based upon the above explanations, it would be completely improper for The Intelligence Group to use a client's computer for anything other than making a bit-stream image of the hard drive. TIG's recommended procedures are:

[1] **John J. Barbara** - Author - General Editor for the "Handbook of Digital & Multimedia Evidence" published by Humana Press in 2007 Published on *Forensic Magazine* (http://www.forensicmag.com) - Computer Forensics Standards and Controls

a. Photograph and document the hardware and remove the hard drive.

b. Create a bit-stream image using a hardware device or software created and tested for this purpose in our lab. In this case, where the drives are encrypted we may need to boot the OS and then create the bit-stream image (using our software) using what is termed a "live acquisition". The bit-stream image is placed on a hard drive purchased by TIG, wiped and formatted in our lab prior to starting the image procedure. This way we know that the hard drive is working and blank prior to starting. The Intelligence Group maintains control of the imaging process by entering all commands, passwords during this process.

c. We then create a backup copy of the bit-stream image on a second drive to be used in the event that the original lab drive malfunctions.

d. We then connect the lab drive containing the bit-stream image to one of our lab computers, where we know the operating system and programs that have been installed. All our forensic processes work with the bit-stream image, but do not change that image in any way. All the results and information from the processes are stored in a separate directory on the same drive. To restate, the bit-stream copy we start with is not changed in any manner during any of our forensic processes.

e. We then run some pre-processes, which is a computer automated search for files that have been deleted and expand compressed files into different evidence files. Compressed files such as ZIP, docx, and tar are files which have been compressed to save space on the hard drive. These files need to be

expanded so that we can conduct searches of their contents. We also search for files and folders which are password protected.

6. In this case, we have been provided with two hard drives and a calculator. The hard drives, according to Mr. Hotz, are encrypted. When an encrypted drive is provided our procedure would be to create a bit-stream copy of the hard drives prior to any other actions or imaging and then create a duplicate of each drive to be utilized for the un-encryption step. This ensures that we always have an "original" bit-stream image of the drives.

7. It is important to explain that a bit-stream image of the hard drive represents a snap shot in time of exactly what was on that hard drive at the time the image was created. This bit-stream image is normally created by a Computer Forensic firm or e-discovery firm when looking for deleted data or providing discovery. However The Intelligence Group was not tasked with providing discovery requests or preservation of data with the exception of documenting and maintaining a copy of any circumvention devices related to a Sony PS3 on the hard drives.

8. The Intelligence Group is only tasked with finding specific data, copying that data into an evidence file and then deleting it from the original hard drive and returning that drive the Mr. Hotz.. Nothing in the order states that we need to maintain a copy of the entire hard drive for discovery or future processing of evidence. During our conference calls Mr. Hotz's attorney has stated several times that there is no reason to keep the bit-stream image of the hard drive as his client is fully capable of maintaining the computer as required in the discovery order. In addition, The Intelligence Group has offered to hold either hold in our evidence an encrypted copy of the bit-stream image or allow Mr. Hotz's attorney to secure this copy of the hard drive in his office as long as would not allow his client access to that drive. Since Mr. Hotz's attorney

has clearly stated that his client is capable of keeping the original hard drive in a manner that does not violate the discovery order, it seemed to me to out of my jurisdiction since I was not tasked with any discovery issues beyond the documentation and storage of circumvention devices related to a Sony PS3.

9. As our role is to be neutral, we had the parties agree to the creating of a bit-stream image after the original drives were placed in the original computer and allowing Mr. Hotz to enter the password so that it would not be known to any party. We would then run the proper processes on our bit-stream image in our lab, create the appropriate copies of the data relating to a circumvention Devices related to a PS3 and finally delete that data off the original hard drive. Once completed we would wipe our bit-stream image of the hard drive. Mr. Hotz's attorney was agreeable to the process but could not allow us to start because a motion was going to be filed requiring The Intelligence Group to preserve the bit-stream image and he knew that Mr. Hotz would not provide his password if any copies were going to be maintained.

10. On February 25th, 2011, we were advised that Mr. Hotz will not agree to allow us to creating any bit-stream image and in addition, we must use his computer for searching and processing.

11. For this forensic examination, I need to confirm that the hard drive does not contain any password protected files. In addition, I need to expand compressed files in order to conduct searches for the circumvention devices related to a PS3. Both of these processes will result in the alteration of data on the original hard drive and even overwrite data that has been previously deleted if ran on the original hard drive. My actions would cause changes and destruction of data to the original hard drive.

12. While we have been told that Mr. Hotz used Linux as the Operating system, I do not how the operating system has been configured, changed or modified. I furthermore do not have any prior knowledge of any traps that may be on the system. While I believe Mr. Hotz to be an honest person and have no reason to suspect that he has made any changes, I will be held accountable if such changes occur. Therefore I am required to assume that all operating systems contain traps and hence must use my lab computers for processing. As an example in one of my forensic classes taught by the White Collar Crime Center, I was able to change the operating system so that when a user typed in the command "copy" it was understood by the system as "format". When any user typed in "Copy C: D:" (which would copy files from drive C to D), the operating system actually ran "Format C:" in such a manner that it would not ask the user if they were sure that they wanted to format the hard drive. Formatting a hard drive overwrites at least the first twenty percent of a 20GB hard drive and removes all files and folders.

13. Therefore, I cannot conduct the searches using the suspect's computer system and operating system. In a perfect world, I would have the complete computer system with the copies of the original hard drives installed along with the password so that I could un-encrypted the drive. However in this case, Mr. Hotz only provided the hard drives, not the computer system and refuses to provide any passwords. Without the original computer system and/or password it is very doubtful that I can un-encrypt the hard drive and proceed as indicated in the court order. I would have been able to proceed with just the hard drives if they were not encrypted.

14. According to Defense counsel, Mr. Hotz is only willing to bring his computer to our location if he can enter the password and TIG will NOT make a copy of the hard drive. Mr. Hotz, will then point out to us that are circumvention devices related to a PS3 and then copy

them off to another drive. Lastly, we must use his computer system and operating system and special tools he has to delete that data off of his hard drive. According to the court order, both parties did agree to have an independent third party conducts the tasks of locating, isolating, segregating and/or removing the information related to Circumvention Devices specific to the Sony PS3 console. In order to accomplish these tasks, TIG will need access to the data, the password and original computer and work in our tested, verified and secure environment.

15. If TIG is not allowed by Mr. Hotz to create a bit-stream image of the hard drive and I am required to use his computer for processing, I will be unable to testify in court that my searches were conducted properly and completely.

16. I am available to testify in person or by phone as requested by either party or the court.

I hereby certify that the foregoing statements made by me are true. I am aware the if any of the foregoing statements made by me are willfully false, I am subject to punishment.

By: _____

Michael Grennier, CFCE, EnCE

Dated: 2/27/2011

EXHIBIT A

CERTIFICAITON of Michael Grennier

CERTIFICATION OF MICHAEL GRENNIER, CFCE, EnCE

I Michael Grennier, CFCE EnCE, of full age and duly sworn, does hereby state as follows:

1. I am the Director of Forensics and Security at The Intelligence Group (TIG), 1545 Route 206, Bedminster, NJ 07921. I have been employed with TIG since January 2008.

2. Prior to my tenure at TIG, I was employed by a computer forensic firm in Princeton, NJ. I started in May 2005 as a Senior Forensic Examiner. Prior to that, I retired as a Police Captain with twenty-five (25) years of service at the South Plainfield Police Department in NJ. Prior to my retirement I had the additional responsibility of maintaining the local government's computer network. As a Police Officer, I worked as a computer forensic examiner on cases involving fraud, theft, and internal affairs investigations, as well as murder, rape, and child pornography. I have received training from Guidance Software, The National White Collar Crime Center and the International Association of Computers Investigative Specialists (IACIS) which include Certified Forensic Computer Examiner (CFCE), Electronic Evidence Collection Specialist (CEECS) and EnCase Certified Examiner (EnCE), Access Data, and Dan Mares Inc. I hold both a Certified Forensic Computer Examiner (CFCE) with IACIS and Encase Certified Examiner (EnCE) certification from Guidance Software. Over the past 12 months I have conducted well over eighty (80) digital forensic examinations.

3. TIG is a digital forensics firm servicing its client's needs in systematically identifying, preserving, extracting, analyzing, and interpreting digital evidence. The firm can uncover e-mail communications, account information, file copying, attempted data destruction, account usage, and other activities performed on computers.

4. TIG has assisted clients in a wide variety of lawsuits, ranging from cases involving fraud, intellectual property theft, wrongful termination, forgery, matrimonial disputes

including child custody and other matters that involve electronically stored information. TIG complies with all computer forensics standards as set forth by the U.S. Federal Bureau of Investigation (FBI) and Guidance Software's Incident Response Forensic Analysis and Discovery (IRFAD) program. The forensic technicians and examiners at TIG employ a number of digital forensic software packages and analysis techniques which include, but are not limited to Guidance Software's EnCase, Access Data's FTK (Forensic Toolkit) and Paraben Software's E-Mail Examiner to complete a comprehensive search of both active and deleted files, as well as to provide an unbiased report of the results. These software products are also utilized by the law enforcement community worldwide. Extensive coursework in the digital forensics field along with hands-on, product-specific training is necessary in order to use these products correctly. Additionally, specialized knowledge and training in chain of custody and evidence handling procedures in the field of digital forensics is necessary in order to perform imaging and analysis up to industry and legal standards TIG's

5. Forensic examinations are never conducted on an original media, device or drive. TIG does not turn on a suspect computer and then search it the way a person sitting in front of the computer might attempt. Our forensic examinations are always undertaken using a "bit-stream" copy. A bit-stream is a copy of the hard drive that captures every bit and byte of data without regard to programs or applications.

6. The Defendant has agreed to bring the same computer which contained and worked with the hard drives that he provided to TIG so that they could be held in evidence as specified in the court order. The importance of this deals with the encrypted hard drives and the operation system drivers which must match the computer hardware for the booting process to successfully occur.

7. In this case, the defendant has represented the hard drives contain a Linux based File and Operating System which he has encrypted by the username and password. In order for the computer to boot and provide TIG access, the defendant will need to either provide TIG the encryption password or enter the password during the boot process. Once the proper password is entered, the data from the hard drive passes to the operating system as unencrypted data. As previously mentioned, the standard procedure would be to create a "bit-stream" image of the hard drive at this time in order for TIG to cost effectively isolate, segregate and/or remove the information on those devices related to Defendant's circumvention devices. For this process to continue, TIG requires a bit-stream image that is verified. For this case, the verification process checks the MD5 hash value of the bit-stream image file to ensure that the data is intact. While it is extremely unlikely that the verification process fails, it does occur in a small percentage of image creations (less than 5%) and requires the process has to be restarted. If the Defendant chooses to enter the password rather than provide that password to TIG, he will be required to stay on-site until the process has been completed and verified because that password may be needed again in the event his computer crashes during this process.

8. Based upon the requested effort, TIG will need to search for and "retrieve" any Circumvention Devices or related information which may include the following areas of the hard drives such as:

a. Active files

b. Deleted files (unallocated space)

c. Slack space (the area between the end of the file and the start of the next cluster or sector)

d. Compressed files including but not limited to TAR, ZIP, TZ etc

e. Password protected files or areas of the hard drive

9. In order to properly conduct the searches and as the rules of evidence provide for, a forensic examiner must be in control of the environment in which the examination is to occur. They must use familiar hardware and software which has been tested and validated. Failure to use properly tested equipment may allow changes to occur to the data and therefore may alter the results. For this reason, the Defendants hard drives can be used to create the bit-stream image only and it should not be used for keyword searches and processing of data.

10. The above explanations were reviewed on a conference call with attorneys and the following protocols were agreed to as stipulated:

a. The Defendant shall bring his computer to TIG offices for the purposes of unencrypting the hard drives.

b. Once the hard drives are installed, the Defendant will enter his password which unencrypts the hard drives.

c. TIG will be allowed to create a bit-stream image of the hard drive for purposes of locating, isolating, segregating and/or removing the information related to Circumvention Devices specific to the Sony PS3 console.

d. After completion of the bit-stream image, the Defendant prior to leaving the offices of TIG, will show TIG the Circumvention Devices and related files specific to the Sony PS3 console so that a file listing can be created.

e. In addition, the Defendant will identify any and all of the following items:

i. Any files, folders or data areas that are encrypted or require a password. Examples would include but not be limited to truecrypt, zip, or rar

ii. Identify if he used or accessed or modified any of the following drive areas ;

1. volume slack
2. Master Boot Record / Superblock
3. Partition table
4. Hosted Protected Area
5. Drive Configuration Overlay
6. Partition slack
7. Sectors or blocks marked as Bad but used to store data
8. Disk slack
9. Unused space in the block group
10. Directory entries

f. The original hard drive will remain in evidence until the Circumvention Devices and related data has been removed.

g. TIG will use portions of data from the Circumvention Devices relating to a Sony PS3 console to search for these devices and/or additional references of circumvention devices across the entire hard drive space .

h. Any Circumvention Devices relating to a Sony PS3 will be documented and stored in a separate evidence file on a hard drive that TIG provides for this purpose.

i. Any code which is questionable as being a Circumvention Device relating to a Sony PS3 console will be reviewed by a TIG sub-contractor that has no conflicts to Sony Corporation. If after this review the code appears to be a

Circumvention Device relating to a Sony PS3 Console, the code will be sent to Mr. Hotz's attorney. Mr. Hotz's attorney will always maintain possession of the code and not allow it to be copied or transferred in any manner. Mr. Hotz is being provided the code so that he can show the code to his client and determine if they want to object to the code being designated as a Circumvention Device. Any objections after a second review by TIG will be brought before the Judge in-camera for the purpose of making a final determination.

j. Once the process of locating the Circumvention Devices relating to a Sony PS3 console have been completed, TIG shall remove the identified data from the original hard drives of Mr. Hotz.

k. Once the identified data has been properly removed from the original hard drives, they shall be returned to Mr. Hotz. once the process of removing the data from Mr. Hotz's hard drives has been completed the bit-stream image of the hard drive shall be wiped. This process will remove all data from that hard drive.

I hereby certify that the foregoing statements made by me are true. I am aware the if any of the foregoing statements made by me are willfully false, I am subject to punishment.

By: 
Michael Grennier, CFCE, EnCE

Dated: 2/26/2011

EXHIBIT 2

Gaudreau, Holly

From: Boroumand Smith, Mehrnaz [mboroumand@kilpatricktownsend.com]
Sent: Friday, February 25, 2011 10:59 AM
To: Stewart Kellar; Robert Kleeger; Michael Grennier
Cc: Gaudreau, Holly
Subject: RE: SCEA v. Hotz - Engagement letter - Final
Attachments: 2011-02-18 (84) Order re Prelim and Hearing on Motion to Dismiss.pdf

Stewart, Robert and Michael,

The purpose of the impoundment is to get the circumvention devices and information related to those devices away from Mr. Hotz. It is not to alter evidence. By having the Intelligence Group retain images of the drives as they originally existed, we can accomplish both the impoundment order and preserve evidence. Moreover, as we discussed on our call, we are amenable to Mr. Kellar, as an officer of the court, maintaining the images once the impoundment is completed while the Court is resolving any discovery disputes.

For your reference, the specific preservation requirement of the preliminary injunction (which was also included in the TRO) is found on page 3 of the attached pdf.

Lastly, the modified order attached by Mr. Kellar regarding the impoundment states that "If there are any disputes between the parties regarding the scope of the information to be segregated and removed from defendants' devices, *or any other disputes* related to the temporary impoundment of the defendant's devices, those matters shall be presented to Magistrate Judge Spero in the first instance." (Emphasis added). Clearly the issue of whether the image of the hard drives is to be deleted is one that needs to be presented to the Magistrate in order to avoid spoliation of evidence. As we discussed on our call, we will raise this issue with Magistrate Judge Spero in a letter copied to each of you early next week.

Thanks,

Mehrnaz

Mehrnaz Boroumand Smith
Kilpatrick Townsend & Stockton LLP
Eighth Floor | Two Embarcadero Center | San Francisco, CA 94111
office 415 273 7559 | fax 415 723 7205
mboroumand@kilpatricktownsend.com | My Profile | VCard

From: Stewart Kellar [mailto:stewart@etrny.com]
Sent: Friday, February 25, 2011 10:12 AM
To: Boroumand Smith, Mehrnaz
Cc: Robert Kleeger; Michael Grennier; Gaudreau, Holly
Subject: Re: SCEA v. Hotz - Engagement letter - Final

Mehrnaz, Rob and Mike,

As a follow up to our call of a few minutes ago, I wanted to make sure that one point was completely clear regarding why the Intelligence Group's wiping of the images made of Mr. Hotz's storage devices (as they exist prior to removal of the circumvention information) is important. The preliminary injunction order clearly carves "isolating, segregating and/or removing [impounded information]" from Mr. Hotz's general requirement to preserve and not destroy evidence. In fact, preservation of the circumvention devices is what is contemplated by the impoundment order. The preliminary injunction reduced the TRO's initial impoundment requirement from impounding the entire drives to merely impounding information related to PS3 circumvention devices and explicitly requires the drives to be promptly returned to Mr. Hotz. No evidence will be destroyed, merely segregated into two parts: the impounded items, and the remaining data on Mr. Hotz's storage devices. Preserving additional images of the devices would violate Judge Illston's Order modifying impoundment for this limited purpose. I have attached the Order for clarity.

Stewart Kellar
E-ttorney at Law™
148 Townsend St. Ste. 2
San Francisco, CA 94107
(415) 742-2303
stewart@etrny.com
www.ettorneyatlaw.com

On Fri, Feb 25, 2011 at 9:56 AM, Boroumand Smith, Mehrnaz <mboroumand@kilpatricktownsend.com> wrote:

> Stewart, Rob and Mike,
>
> As a follow up to our call of a few minutes ago, I wanted to make sure that one point was completely clear regarding why the Intelligence Group's preservation of the images made of Mr. Hotz's storage devices (as they exist prior to removal of the circumvention information) is important. If the images are wiped by the Intelligence Group after the impoundment procedure is completed (and the impounded information is removed), no one, including Mr. Hotz, will have a forensically intact copy of his hard drives as they existed originally. Consequently, evidence of the hard drives in their original form -- clearly relevant to the merits of this case -- will be destroyed in violation of the Court's TRO and preliminary injunction orders.
>
> Thanks,
>
> Mehrnaz
>
> **Mehrnaz Boroumand Smith**

EXHIBIT 3

Boroumand Smith, Mehrnaz

From: Michael Grennier [MGrennier@intell-group.com]
Sent: Saturday, February 26, 2011 6:33 PM
To: Boroumand Smith, Mehrnaz; Gaudreau, Holly; Robert Kleeger; Stewart Kellar
Cc: Robert Kleeger
Subject: RE: Certification for review

Mehrnaz,

See below:

From: Boroumand Smith, Mehrnaz [mboroumand@kilpatricktownsend.com]
Sent: Saturday, February 26, 2011 8:04 PM
To: Michael Grennier; Gaudreau, Holly; Robert Kleeger; Stewart Kellar
Subject: RE: Certification for review

Dear Michael,

Thanks for sending the draft protocols.

Late yesterday, Mr. Kellar informed us that Mr. Hotz would not allow any imaging of his hard drives to occur. Based on our call, we understood that he would be updating you on Mr. Hotz's position (including an alternative proposal that was not acceptable to SCEA). Consequently, we are in the process of putting together a joint dispute letter that the parties will file with the Court on Monday morning.

For our part, we would like to present the court with your proposed protocol subject to the following clarifications and comments:

1. We believe you may have inadvertently left out the initial step of creating forensic bit-stream images of the devices provided by Mr. Hotz. As you stated in paragraph 5 of the protocols and we understand from our forensics consultants, original media, devices or drives are never used to conduct examinations because of concerns, including among others, that the original hard drives may fail. Consequently, we believe that two such images should also be made here – one to be maintained in a secure vault by the Intelligence Group and the second to be used for decryption (rather than using the original hard drive). Please confirm that under your suggested protocol, the Intelligence Group would create such images and if not, let us know why not.
Section 10.C clearly states that we will be creating a bit-stream image of the hard drive. As for two images, that was not agreed to during our conversations. In additon, we would still have to wipe both copies at the end.
I would agree that two images would be the "norm" and provide a back-up in the event the primary drive fails, but it was not agreed to by the parties and based on the last email they are now not agreeing to the what we discussed and agreed to during the phone call..

Similarly, please confirm that two bit-stream forensic images of the decrypted hard drive will be created – one for preservation purposes (to be maintained in a secure vault at the Intelligence Group until such time as the Court resolves the protocol and discovery disputes between the parties) and the second to conduct your review with Mr. Hotz as well as your independent searches and analysis.
IF there was an agreement to maintain a preserved copy, then the proper proceedure would be to create a bit-stream (forensic) image of the drives while encrypted and prior to starting these processes. Then create a second bit-stream (forensic) image after the drive was unencrypted with the password. This would provide us with a before and after data for court purposes that I could present if requested by either party. However there is no agreement to maintaining a copy for preservation of the hard drive and even a requirement that we wipe our data copies upon completion. In addition Mr. Holtz Attorney has clearly stated that it is his intention and belief that there is no need for him to have a copy or maintin a copy of the hard drive and he is of the belief that his client is capable of keeping the data intact as required under the discovery order.

Also please confirm that the working bit-stream image of the decrypted hard drive (and not the original device provided by Mr. Hotz) will be used for analysis. We do not want Mr. Hotz to contend that the Intelligence Group has in any way altered the original hard drive except at the very end of the analysis when you remove the information and devices related to circumvention that you have located (through your analysis on the working copy) from the original devices provided by Mr. Hotz.
The Intelligence Group has stated in the certification that we will be createing a bit-stream image of the un-encrypted drive. We will use our copy of the bit-stream image to locate and document the devices related to circumvention. Then we will remove the data from those areas of the original hard drive as the last step. THE INTELLIGENCE GROUP IS UNABLE AND UNWILLIG TO USE HIS COMPUTER FOR ANYTHING OTHER THAN OBTAINING A BIT-STREAM COPY OF THE UNENCRYPTED DRIVE.

2. Please confirm that under your protocols for chain of custody purposes you will photograph both original hard drives as well as document the drives' model and serial numbers and record BIOS or other system clock information.
The Original drives were photographed and a Chain of Custory was completed and signed by Goerge Holtz's dad who dropped them off at our offices. A copy can be forwarded on Monday if requested. We also have the drives make and model on file. When the comptuer is presented we will record the BIOS information, along with the time/date on the bios Clock.

As we have to provide our response to the Joint Discovery letter to Mr. Kellar by 4 pm PT tomorrow, we ask that you respond to our questions by no later than noon your time tomorrow.

We greatly appreciate your assistance over the weekend on this matter.

Mehrnaz

Mehrnaz Boroumand Smith
Kilpatrick Townsend & Stockton LLP
Eighth Floor | Two Embarcadero Center | San Francisco, CA 94111
office 415 273 7559 | fax 415 723 7205
mboroumand@kilpatricktownsend.com | My Profile | VCard

From: Michael Grennier [mailto:MGrennier@intell-group.com]
Sent: Saturday, February 26, 2011 7:37 AM
To: Gaudreau, Holly; Robert Kleeger; Stewart Kellar; Boroumand Smith, Mehrnaz
Subject: Certification for review

Attached is my certification in draft form for reivew. Please comment and advise. I will forward the final copy with signatures by Sunday evening.

Regards,

Mike

EXHIBIT 4

Boroumand Smith, Mehrnaz

From: Michael Grennier [MGrennier@intell-group.com]
Sent: Saturday, February 26, 2011 7:02 PM
To: Stewart Kellar
Cc: Gaudreau, Holly; Robert Kleeger; Boroumand Smith, Mehrnaz
Subject: RE: Certification for review

Mr. Keller,

I am sadden to hear that you will no longer agree with the process agreed to by you on Friday. While the court would need to decide the issue of the preservation. I felt that the Intelligence Group was working as neutral in getting the process on paper and you were working with all parties by agreeing to allow the drive to be imaged and having it wiped at the end of the process.

I need to state and will now include in a second certification that you did agree to the steps listed in the first certification, but after consulting with your client they are no longer acceptable. In additon I can only use Mr. Holtz's computer to create the unencrypted bit-stream image file. I can not use his software or his computer to search for data to be wiped. His computer is unknown and untested in my environment. I can't even use standard Unix commands without knowing or having a way to confirm that they are working properly under test conditions. While it is not plausible, it is possible that the OS could have been changed so that a copy command is now a format command or that the standard command line entries work different due to changes made in the OS. I also completely disagree with your statement that this is not a forensic examination. I am being task to search for, and locate data on a hard drive even data that my have been deleted using standard forensic techniques. My review of the Court Order does not indicate that your client has sole responsibility to search for and "point out" the Circumvention devices and supervise the deletion. Rather it is my reading that I as the independent third party am responsible for making that determination and then removing the data from the original hard drive.

I also want to state that The Intellignece Group fully expects both parties to pay for the professional services provided by such as the accepting of the hard drives, conference calls and writting of certifications as agreed to. I am sure and please confirm that your statement that Mr. Hotz will provide The Intelligence Group with our intiial retainer being listed in the agreement to an alternate proposal pargraph was just information included in that paragraph rather than a threat to withhold payment during this process if the other side did not agree with your proposal.

I understand that everyone is under deadlines, and I will try to have my second certification to you by tomorrow noon. The First certification will be signed as is and forwarded by Sunday Evening.

Regards,

Mike

From: Stewart Kellar [stewart@etrny.com]
Sent: Saturday, February 26, 2011 8:35 PM
To: Michael Grennier
Cc: Gaudreau, Holly; Robert Kleeger; Boroumand Smith, Mehrnaz
Subject: Re: Certification for review

Mr. Grennier,

We will not agree to allow any image or copy to be made of Mr. Hotz's drives or allow searches to be run on Mr. Hotz's drives using systems and programs not native to Mr. Hotz's computer system. The Impoundment order calls

for impoundment only. It is not a forensic examination and does not require that imaged copies of Mr. Hotz's storage devices be made. Thus, any imaging or additional copies of Mr. Hotz's drives goes beyond the scope of the impoundment order and beyond the scope of the how Mr. Hotz's drives may be access and/or manipulated.

As an alternate proposal, Mr. Hotz agrees that on Monday February 28, 2011, he will go to your office and provide you with the initial retainer and fully signed agreement. Mr. Hotz then agrees to demonstrate that the circumvention devices at issue are indeed on the impounded devices. Mr. Hotz agrees to bring his computer system which will be used to access the drives and identify the circumvention devices therein. After the devices are shown to have the circumvention devices, they will be left impounded in your office's custody until such time the court either lifts the impoundment order or makes an order otherwise affecting the impounded drives.

I contacted SCEA's counsel at 3:02pm PST yesterday to discuss our proposal, and left a message. The call was returned by SCEA's counsel at 5:00pm PST who ultimately stated their opposition to our alternate proposal. Both parties have agreed to a schedule for drafting a joint letter to Magistrate Judge Spero on the matter, which will be filed and submitted to the Judge by Monday, February 28th.

The statements made in your draft letter do not reflect our position and are not agreed to. I look forward to receiving a revised draft that reflects our position in this matter. Thank you.

Sincerely,

Stewart Kellar
E-ttorney at Law™
148 Townsend St. Ste. 2
San Francisco, CA 94107
(415) 742-2303
stewart@etrny.com
www.ettorneyatlaw.com

On Sat, Feb 26, 2011 at 7:37 AM, Michael Grennier <MGrennier@intell-group.com> wrote:

> Attached is my certification in draft form for reivew. Please comment and advise. I will forward the final copy with signatures by Sunday evening.
>
> Regards,
>
> Mike

EXHIBIT 5

Volume 1

Pages 1 - 36

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

BEFORE THE HONORABLE SUSAN ILLSTON, JUDGE

SONY COMPUTER ENTERTAINMENT AMERICA, LLC, Plaintiff, VS. GEORGE HOTZ, ET AL., Defendants.	 COPY NO. C 11-00167 SI San Francisco, California Thursday February 10, 2011 10:29 a.m.

TRANSCRIPT OF PROCEEDINGS

APPEARANCES:

For Plaintiff:
KILPATRICK TOWNSEND
Two Embarcadero Center
Eighth Floor
San Francisco, California 94111
BY: JAMES G. GILLILAND, JR., ESQ.
HOLLY GAUDREAU, ESQ.
RYAN BRICKER, ESQ.

For Defendant George Hotz:
LAW OFFICES OF STEWART KELLAR
148 Townsend Street
Suite 2
San Francisco, California 94107
BY: STEWART KELLAR, ESQ.

Also Present: MICHAEL EDELMAN

Reported by: BELLE BALL, CSR #8785, RMR, CRR
Official Reporter, U.S. District Court

stand at the podium at the same time, if you want.

MR. KELLAR: Thank you.

With regard to allowing Sony access to my client's computer to inspect all files to find out which ones are and are not the circumvention devices again raises the same issue of impounding Mr. Hotz's privileged, confidential, and otherwise private information on his computers.

THE COURT: And, you know why that issue comes up? Because that's where he did what he did. And for present purposes, anyway, what he did was not all right. So, --

MR. KELLAR: That's correct, Your Honor.

THE COURT: -- that's the breaks.

MR. KELLAR: However, the TRO already states that Mr. Hotz is to preserve and not destroy any records or documents in whatever format relating to the circumvention devices, and Mr. Gilliland has -- or Sony's counsel has demonstrated no risk of spoliation, of covering tracks, of any illicit activity involving tampering with evidence after receiving notice of this suit.

THE COURT: Oh, I don't think that's right. I got something just yesterday or the day before that he's posted -- posted things on the Internet that is in direct violation of the order.

MR. KELLAR: It is not correct that he posted things in direct violation of the order. He posted a link to