

1 KILPATRICK TOWNSEND & STOCKTON LLP
 JAMES G. GILLILAND, JR. (State Bar No. 107988)
 2 TIMOTHY R. CAHN (State Bar No. 162136)
 MEHRNAZ BOROUMAND SMITH (State Bar No. 197271)
 3 HOLLY GAUDREAU (State Bar No. 209114)
 RYAN BRICKER (State Bar No. 269100)
 4 Two Embarcadero Center Eighth Floor
 San Francisco, CA 94111
 5 Telephone: (415) 576-0200
 Facsimile: (415) 576-0300
 6 Email: jgilliland@kilpatricktownsend.com
 tcahn@kilpatricktownsend.com
 7 mboroumand@kilpatricktownsend.com
 hgaudreau@kilpatricktownsend.com
 8 rbricker@kilpatricktownsend.com

9 Attorneys for Plaintiff
 SONY COMPUTER ENTERTAINMENT AMERICA LLC

10
 11 UNITED STATES DISTRICT COURT
 12 FOR THE NORTHERN DISTRICT OF CALIFORNIA
 13 SAN FRANCISCO DIVISION

14 SONY COMPUTER ENTERTAINMENT
 AMERICA LLC,

15 Plaintiff,

16 v.

17 GEORGE HOTZ; HECTOR MARTIN
 18 CANTERO; SVEN PETER; and DOES
 19 1 through 100,

20 Defendants.

Case No. 11-cv-00167 SI

**[PROPOSED] ORDER RE
 MARCH 10, 2011 TELEPHONIC
 HEARING RE JOINT LETTER ON
 IMPOUNDMENT ISSUES AND JOINT
 LETTER ON DISCOVERY**

21
 22
 23 On March 10, 2011, the Court held a hearing on the parties' February 18, 2011 and
 24 February 28, 2011 joint letters (Docket Nos. 85 and 86) on discovery and impoundment
 25 disputes. Having considered all the papers and arguments, the Court enters the following
 26 order:

27 (1) Plaintiff SCEA is authorized to serve third party PayPal, Inc. with a subpoena
 28 seeking the following limited information relating to personal jurisdiction: documents sufficient

1 to identify the source of funds in California that went into any PayPal account associated with
2 geohot@gmail.com for the period of January 1, 2009 to February 1, 2011. SCEA is ordered
3 to redraft its subpoena to seek this information. SCEA is further ordered to inform PayPal,
4 Inc. and other subpoenaed parties that any information produced in response to the
5 subpoena shall be provided on an Attorneys' Eyes Only basis and that the issuance of the
6 subpoena is without prejudice to its right to file a Motion to Quash. (See Docket No. 92)

7 (2) Mr. Hotz is ordered to sign a consent for SCEA to obtain his Twitter posts from
8 January 1, 2009 to the present.

9 (3) Defendant George Hotz is ordered to appear in California for a deposition
10 relating solely to the question of personal jurisdiction. SCEA shall pay reasonable expenses
11 of Mr. Hotz to be deposed in California. The parties shall determine the date of the
12 deposition. Additionally, the parties have stipulated that Mr. Hotz cannot be served with
13 process by the parties to this action or the parties identified in SCEA's Certification of
14 Interested Entities or Person (Docket No. 16) when he appears at his personal jurisdiction
15 deposition in California.

16 (4) With regard to the impoundment, the Court orders that:

17 (a) The Intelligence Group ("TIG"), the third party neutral chosen by both parties,
18 shall only take steps with regard to the impounded devices that are authorized by
19 Court order.

20 (b) The first \$7000 of TIG costs will be split equally between SCEA and Mr. Hotz.
21 SCEA has agreed to and shall pay any amount over the \$7000.

22 (c) TIG is ordered to conduct the impoundment in the forensically sound manner as
23 proposed in its Certification of February 27, 2011, including Exhibit A to that
24 certification. Attached hereto as Exhibit 1 is a true and correct copy of the
25 February 27, 2011 Certification and Exhibit A.

26 (d) Judge Illston's modified impoundment order requires the isolation, segregation
27 and/or removal of information related to Defendant Hotz's circumvention of the
28 technological protection measures in the PS3 System. The Court orders the

1 parties and TIG to meet and confer regarding what exactly is information related
2 to the circumvention of the technological protection measures in the PS3 System
3 and a procedure to isolate, segregate and remove such information. The parties
4 shall submit a description of the protocol to the Court for entry into an order by no
5 later than March 28, 2011.

6 (5) With regard to jurisdictional discovery of the impounded devices, the Court
7 orders that:

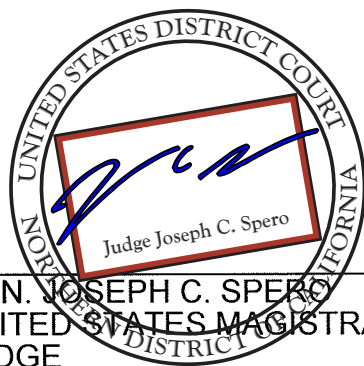
8 (a) In order to avoid conducting discovery searches on original impounded devices
9 belonging to Mr. Hotz, TIG shall make an additional copy of both the encrypted and
10 unencrypted versions of the impounded hard drives and keep them in their
11 possession.

12 (b) TIG shall then conduct a forensically sound search of the impounded devices to
13 determine whether: (i) they contain all or portions of the development tools for the
14 PlayStation 3 System and (ii) the impounded devices have been used to access or
15 connect to the PlayStation Network. The Court orders the parties and TIG to meet
16 and confer on a protocol for TIG to perform these searches. The parties shall
17 submit a description of the protocol to the Court for entry into an order by no later
18 than March 16, 2011.

19 (6) The parties shall enter a Stipulated Protective Order for all discovery matters.
20 To the extent the parties are unable to agree on the terms, they are ordered to file a joint
21 letter no longer than ^{three (3) - JCS} ~~10~~ pages to set forth the disputed terms and the parties' respective
22 positions.

23
24 **IT IS SO ORDERED.**

25
26 DATED: 03/15/11



27
28 HON. JOSEPH C. SPERO
UNITED STATES MAGISTRATE
JUDGE

63207604 v1

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 as 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 know 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 arc circumvention devices related to a PS3 and then copy

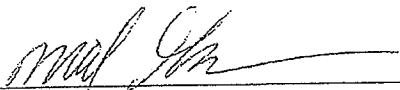
them off to another drive. Lastly, we must use his computer system and operating system and special tools he has to delete that data off of his hard drive. According to the court order, both parties did agree to have an independent third party conducts the tasks of locating, isolating, segregating and/or 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.

Michael Grennier, CFCE, EnCE

By:  _____

Dated: 2/27/2011

EXHIBIT A

CERTIFICATION 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 ;

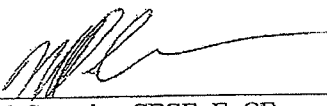
1. volume slack
2. Master Boot Record / Superblock
3. Partition table
4. Hosted Protected Area
5. Drive Configuration Overlay
6. Partition slack
7. Sectors or blocks marked as Bad but used to store data
8. Disk slack
9. Unused space in the block group
10. Directory entries

- 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:

2/29/2011