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

Attorneys for Plaintiff
SONY COMPUTER ENTERTAINMENT AMERICA LLC

UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

SONY COMPUTER ENTERTAINMENT AMERICA LLC,

Plaintiff,

v.

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

Defendants.

Case No. 11-cv-00167 SI

[PROPOSED] ORDER RE PROTOCOL FOR JURISDICTIONAL DISCOVERY ON IMPOUNDED DEVICES

On March 10, 2011, the Court ordered plaintiff Sony Computer Entertainment America LLC ("SCEA"), Defendant George Hotz ("Hotz"), and the third party neutral, The Intelligence Group ("TIG"), to meet and confer on a protocol for the search of the impounded devices to determine whether: (1) they contain all or portions of the development tools for the PlayStation® 3 System ("PS3 System") and (2) the impounded devices have been used to

access or connect to the PlayStation Network ("PSN"). On March 16, 2011, the parties submitted competing protocols together with a Joint Letter Related to Jurisdictional Search of Mr. Hotz's Impounded Hard Drives (Docket No. 98) to the Court. On March 28, 2011, the Court held a Telephonic Discovery Conference regarding the Joint Letter. Having reviewed the papers and heard arguments from the parties, the Court orders as follows:

(1) TIG will forensically image the impounded devices in their encrypted state.

(2) Mr. Hotz shall make himself available to TIG on or before April 1, 2011 to provide TIG access to his computer and passwords for the purpose of creating un-encrypted images of the devices. Mr. Hotz shall make himself available to TIG until the process is completed.

(3) Counsel for SCEA shall provide to TIG copies of the following items which will be copied into evidence files:

(a) A copy of the PS3 System Software Development Kit ("SDK")

(b) A list of URLs and cookies and other information agreed upon by the parties which might appear on a user's computer if they accessed the "secure" area of the PSN which requires a valid user name and password ("PSN Secure Area")

(4) SCEA shall make the SDK available for review by Mr. Hotz's outside counsel for record in this action under the following conditions:

(a) Mr. Hotz's outside counsel of record ("Qualified Persons") may review the SDK at SCEA counsel's office at Kilpatrick Townsend and Stockton LLP in San Francisco on a "stand alone" secure computer system (i.e. the computer system will not be linked to any network, including a local area network ("LAN"), an intranet or the Internet). Qualified Persons shall sign a Non-Disclosure Agreement before reviewing the SDK.

(b) No recordable media or recordable devices, other than those physically installed in a computer or cell phone, shall be permitted into the area containing the stand alone computer system, including without limitation sound recorders, peripheral equipment, cameras, CDs, DVDs, or drives of any kind. No computers, recordable media, or recordable devices may be connected to any such stand-alone secure computer system or otherwise

used to copy or record the SDK from such stand-alone secure computer system. No means capable of connecting computers, recordable media, or recordable devices to the stand-alone secure computer system shall be permitted into the area and no computers may be used to duplicate or re-write any portions of the SDK.

(c) The stand alone secure computer system shall be password protected.

(d) Counsel for SCEA shall provide the password and the SDK to Qualified Persons, who will then be allowed to insert the SDK in the stand alone secure computer system.

(e) Qualified Persons may not alter, dismantle, disassemble or modify the stand alone secure computer system or the SDK in any way, or attempt to circumvent any security feature of the stand alone secure computer system or the SDK in any way.

(f) No copies shall be made of the SDK, whether physical, electronic, or otherwise. Qualified Persons may take notes of his thoughts and impressions during any review of the SDK. Any notes concerning the SDK shall not be used to circumvent the restrictions herein against making copies of the SDK. Persons viewing the notes shall do so in a manner consistent with restrictions on material designated as HIGHLY CONFIDENTIAL – OUTSIDE ATTORNEY'S EYES ONLY INFORMATION.

(5) Counsel for the parties shall review and agree to search terms that TIG shall use to conduct searches in an effort to prove or disprove access to the PSN Secure Area. These agreed upon terms will be provided to TIG no later than April 1, 2011. Lead counsel for the parties shall meet and confer in person to determine these search terms.

(6) Counsel for the parties shall review and agree to search terms that TIG shall use to conduct searches on any SDK material found on the devices. These agreed upon terms will be provided to TIG no later than April 1, 2011. Lead counsel for the parties shall meet and confer in person to determine these search terms.

(7) TIG shall review the URLs and cookies provided by counsel for SCEA and verify that the sites are located on the PSN Secure Area.

(8) Once the forensic images of the un-encrypted drives have been pre-processed, TIG shall conduct the following procedures:

(a) TIG shall search the devices for URLs and cookies, and other information agreed upon by the parties in an attempt to prove or disprove that the computer system had accessed the PSN Secure Area.

(b) TIG shall conduct keyword searches as agreed to by both parties in an effort to prove or disprove that the computer system had accessed the PSN Secure Area.

(c) TIG shall search the devices and determine if all or any portion of the SDK provided to TIG by SCEA exists on the devices.

(d) TIG shall search all or any portion of the SDK that is found on the devices with additional search terms agreed to by the parties.

(9) TIG shall provide the results of the searches to counsel for Mr. Hotz on or before April 5, 2011. Counsel for Mr. Hotz shall review this data and provide counsel for SCEA with a privilege log, on or before April 11, 2011**,** containing sufficient information so that counsel for SCEA may be able to determine if the information is privileged. Other than material as to which a privilege has been asserted, the results of these searches and processes shall be produced to counsel for SCEA on or before April 11, 2011. This production shall be designated as HIGHLY CONFIDENTIAL – ATTORNEYS' EYES ONLY, and treated as such by both parties, except that Mr. Hotz shall be permitted to review this production for purposes of his defense in this lawsuit.

(10) Mr. Hotz shall appear for his deposition in California on April 15, 2011.

(11) This Court shall recommend to the Honorable Susan Illston the following revised schedule for supplemental briefing and for the hearing date for Mr. Hotz's Motion to Dismiss for Lack of Personal Jurisdiction and Improper Venue:

Supplemental briefing filed by SCEA:	April 20, 2011
Reply filed by Mr. Hotz:	April 22, 2011
Hearing on Motion to Dismiss:	May 6, 2011 or as soon thereafter as is convenient for Hon. Susan Illston.

///

///

IT IS SO ORDERED.

DATED:_____

_____
HON. JOSEPH C. SPERO
UNITED STATES MAGISTRATE JUDGE

63232294 v1