

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

15 SONY COMPUTER ENTERTAINMENT
 AMERICA LLC,

16 Plaintiff,

17 v.

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

20 Defendants.
 21

Case No. 11-cv-00167 SI

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

22
 23
 24 On March 10, 2011, the Court ordered plaintiff Sony Computer Entertainment America
 25 LLC ("SCEA"), Defendant George Hotz ("Hotz"), and the third party neutral, The Intelligence
 26 Group ("TIG"), to meet and confer on a protocol for the search of the impounded devices to
 27 determine whether: (1) they contain all or portions of the development tools for the
 28 PlayStation® 3 System ("PS3 System") and (2) the impounded devices have been used to

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

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

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

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

13 (a) A copy of the PS3 System Software Development Kit (“SDK”)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

23 Supplemental briefing filed by SCEA: April 20, 2011

24 Reply filed by Mr. Hotz: April 22, 2011

25 Hearing on Motion to Dismiss: May 6, 2011 or as soon thereafter as is
26 convenient for Hon. Susan Illston.

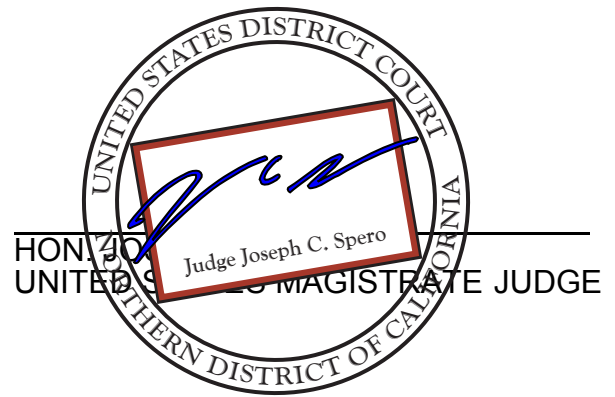
27 ///

28 ///

1 **IT IS SO ORDERED.**

2
3
4 DATED: 03/29/11

5
6 63232294 v1



7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28