YASHA HEIDARI (GA Bar No. 110325)
yasha@hplawgroup.com
Heidari Power Law Group LLC
PO Box 79217
Atlanta, Georgia 30357

STEWART KELLAR (SBN 267747)
stewart@etrny.com
E-ttorney at Law
148 Townsend Street, Suite 2
San Francisco, California 94107
Telephone: (415) 742-2303

JACK C. PRAETZELLIS (SBN 267765)
jack@mbvlaw.com
MBV LAW LLP
855 Front Street
San Francisco, California 94111
Telephone: 415-781-4400
Facsimile: 415-989-5143

Attorneys for Defendant George Hotz

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

SONY COMPUTER ENTERTAINMENT AMERICA LLC, a Delaware limited liability company,

Plaintiff,

v.

GEORGE HOTZ, et al.,

Defendants.

Case No. 11-CV-000167 SI

DECLARATION OF ALEXANDER STAMOS IN REPLY TO SCEA'S OPPOSTION TO DEFENDANT HOTZ'S MOTION TO DISMISS

I, Alexander Stamos, declare:

1. I am of required age and competent in all respects to testify regarding the matter set forth herein. I am a Vice President and Chief Technical Officer at iSEC Partners, an agent for counsel of record for defendant George Hotz in the above-captioned matter. The relationship between iSEC Partners and Stewart Kellar is governed by a mutual nondisclosure agreement to provide eDiscovery, data analysis, and project support upon request. I have personal knowledge of the facts stated herein and know them to be true. And if called as a witness could and would testify competently thereto.

2. iSEC Partners (iSEC) is an information security consulting firm headquartered in San Francisco, with offices in Seattle and New York. Our work includes software assurance, infrastructure penetration testing, code review, incident response and forensics. Our clients include Microsoft, Oracle, eBay, McKesson, Salesforce.com, Google, Autodesk, Charles Schwab, JPMorgan Chase, Bank of America, Wells Fargo, ING Direct and Motorola.

3. I am a co-founder of iSEC Partners, which we formed in October 2004. Before founding iSEC Partners I worked as a Managing Security Consultant with the security consultancy @stake, and I was the security lead at Loudcloud, a managed hosting provider. I have also worked for the EO Lawrence Berkeley National Laboratory. I hold a BS in Electrical Engineering and Computer Science from the University of California, Berkeley, where my studies included graduate classes in networking and computer security. I was awarded a Certified Information Systems Security Professional (CISSP) certification in April 2003. I am a frequent speaker at leading security and technology conferences, such as Black Hat USA, CanSecWest, Microsoft BlueHat, the Web 2.0 Expo, CTIA, OWASP App Sec, and the Financial Services Information Sharing and Analysis Center (FS-ISAC). I have also spoken on the topic of computer forensics to private audi-

ences at the FBI's Regional Computer Forensics Laboratory, and the Federal Reserve Banks in New York and Boston.

4. On Thursday, March 24, 2011 iSEC Partners was contracted to perform a technical analysis of raw data weblogs provided by BlueHost, Inc. Specifically, we were asked to isolate log entries that listed <geohot.com> or a subdomain and included a request for "jailbreak.zip"

5. On March 24, 2011 iSEC Partners received this data on a USB Flash Drive from Stewart Kellar at our San Francisco office. The log data was copied to several secure workstations for analysis by myself and two colleagues under my direction and supervision. All of our work was done with standard UNIX text manipulation and search commands, such as grep, awk, find and sort.

6. We decompressed the provided files and separated out the logs for applications other than the <geohot.com> web server. We then created a temporary file containing only requests involving the "jailbreak.zip" file.

7. We examined this temporary file for all possible HTTP methods and identified four in use: HEAD, GET, POST, and OPTIONS. As GET and POST are the only two requesting methods for which the jailbreak.zip data will be returned, we extracted only requests using these two methods into a new intermediate file. From here we were able to split the file according to response code and calculate the total number of requests.

8. We found that a grand total of **1,136,409** requests were made globally for jailbreak.zip, not accounting for unique IPs. Over the entire period covered by these logs **323,518** global unique IP addresses successfully downloaded jailbreak.zip.

9. We also separated the requests based upon the time periods in Mr. Bricker's declaration. We condensed down the requests to unique IPs seen in each time period for each response, meaning that uniqueness of IPs was not enforced globally. We believe this to be the criteria used by Mr. Pierce as best we can determine from his declaration. Using this criteria, we found the number of IPs that attempted to download jailbreak.zip from <geohot.com> to be:

a. 1/8/2011 – 1/12/2011: **162,510** unique IPs requested jailbreak.zip (**1,659** were unsuccessful, **160,851** were 200, 206 or 304 downloads)

b. 1/13/2011 – 1/27/2011: **217,411** unique IPs requested jailbreak.zip (**4,003** were unsuccessful, **213,408** were 200, 206 or 304 downloads)

c. 1/28/2011 – 3/7/2011: **96,408** unique IPs requested jailbreak.zip (**96,407** returned HTTP Code 404, unsuccessful downloads and **1** request returned Code 200. We believe this to be an anomaly caused by a malformed request and not a successful download of jailbreak.zip)

10. The numbers in 9a, 9b, and 9c above do not sum up to the number of global unique IPs specified in paragraph 8 due to the ordering of operations to match the Pierce declaration.

11. In the Declaration of Ryan Bricker, I understand that Mr. Bricker considered HTTP codes 200, 206, and 304 to be "successful downloads" of jailbreak.zip from <geohot.com>. According to the specification of the Hypertext Transfer Protocol version 1.1 (HTTP 1.1), codified in RFC 2616 <http://www.rfc-editor.org/rfc/rfc2616.txt>, only response codes of the 2XX family are consider "successful", where "This class of status code indicates that the client's request was successfully received, understood, and accepted." The 304 response indicates that the requested resource was "Not Modified" and the specification states "The 304 response MUST NOT contain a message-body". This means that this response could not have contained any portion of the jailbreak.zip file and should not be counted as a successful download of the file. Nevertheless, we have included 304 responses in our count above for comparability with Mr. Bricker's declaration.

12. We delivered our results from analyzing these logs in an Excel spreadsheet delivered to Mr. Kellar, attached here as Exhibit A.

I declare under penalty of perjury on this date under the laws of the United States of America in San Carlos, California that the foregoing is true and correct.

Dated: March 25, 2011.

Alexander Stamos, VP and CTO

4841-7608-3208, v. 2