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, 8th Floor
San Francisco, California 94111
Telephone: (415) 576-0200
Facsimile: (415) 576-0300
Email: jgilliland@kilpatricktownsend.com
tcahn@kilpatricktownsend.com
mboroumand@kilpatricktownsend.com
hgaudreau@kilpatricktownsend.com
rbricker@townsend.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, a Delaware limited liability company,

Plaintiff,

v.

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

Defendants.

Case No. CV11-0167 SI

DECLARATION OF BRET MOGILEFSKY IN SUPPORT OF *EX PARTE* MOTION FOR TEMPORARY RESTRAINING ORDER AND ORDER TO SHOW CAUSE RE PRELIMINARY INJUNCTION; ORDER OF IMPOUNDMENT

Judge: Hon. Susan Illston

I, Bret Mogilefsky, declare:

1. I am employed full-time as a Senior Manager of Developer Support at Sony Computer Entertainment America LLC ("SCEA"), a position I have held since August of 2003. My responsibilities include oversight of engineering and technical operations in support of partner development. I have personal knowledge of the facts stated in this declaration, unless otherwise indicated, and could and would testify competently thereto.

A. PlayStation®3 Computer Entertainment System

2. The PlayStation®3 computer entertainment system is a home entertainment system featuring hardware and firmware designed for the playing of video games (collectively "the PS3 System"). Firmware is a fixed program or data structure that internally controls various electronic devices.

3. SCEA's video games for the PS3 System and all video games validly licensed to be played on the PS3 System are programmed with computer code, referred to herein as the "PlayStation3 Programmer Tools," that authenticate authorized video game software and permit it to interact with the central processing unit and microprocessors in the PS3 System. A video game whose code does not incorporate the PS3 Programmer Tools cannot be played on the PS3 System. The PS3 Programmer Tools are also incorporated within the PS3 System firmware.

B. Technological Protection of PS3 System Video Game Software

4. All genuine PS3 Systems are manufactured with technological protection measures ("TPMs") that effectively control access to the PS3 System, prevent unauthorized access, copying and/or decryption of the PS3 Programmer Tools, prevent unauthorized or unlicensed software from playing on the PS3 System, and prevent users from running infringing copies of video games and/or firmware code.

5. The PS3 System is designed to run multiple levels of authorized, encrypted code in one or more sequences. Each level features TPMs, which control access, encrypt and decrypt code, and authenticate signatures to ensure the user has proper authorization to access the files within the code.

6. The TPMs in the PS3 System are designed to allow only the operation of legitimate, authorized and approved software that is licensed for distribution in the region or geographical territory of the console's sale.

7. For example, the TPMs in the PS3 System are designed to prevent users from running code such as Defendant George Hotz's "3.55 Firmware Jailbreak."

8. The TPMs in the PS3 System include, but are not limited to, the following features:

(a) the encryption of Bluray Disc content;

(b) firmware which is commercially valuable to SCEA can only be installed on the internal hard drive and integrated circuit chips, which means that such firmware cannot be decrypted, transferred to external storage devices, and shared freely;

(c) the internal hard drive is encrypted, which means that data on a PS3 System 's hard drive is protected by an encryption key unique to that PS3 System; and

(d) video games for the PS3 System are protected by digital rights management, which prevents unauthorized parties from accessing them.

9. Among its other TPMs, the PS3 System uses an "Elliptic Curve Digital Signature Algorithm" ("ECDSA") security system. The ECDSA system uses an algorithm to generate "signatures," which are applied to every file authorized to run on the PS3 System, including files that boot or read a video game disc, for example. If a file or program does not contain a valid digital signature, the PS3 System will not run that file or program. These signatures are also encrypted.

10. Each signature is generated using a pair of electronic Keys ("Keys"), including a "private key" and a "public key." The private Keys are held by SCEA; they are not distributed, and they cannot be found anywhere in the PS3 System's code, in its hardware, or in the code of any authorized application or video games. The public Keys that correspond to each piece of code are encrypted and embedded on stable processing elements that are isolated from the user by SCEA's TPMs during normal use of the PS3 System. SCEA uses these Keys to digitally authenticate code before it can be run on any

level of the PS3 System. The PS3 System verifies each ECDSA signature by decrypting and inserting the signature into an algorithm along with the appropriate public key, solving the equation, and ensuring that the algorithm has produced the correct values. The PS3 System will not execute a file unless that file contains an authentic signature.

11. Unauthorized, unlicensed, or copied video game discs do not have a valid digital signature. Accordingly, a normally-functioning PS3 System will not run those pirated games.

12. In order to run code and/or execute files at various levels of the PS3 System, an individual must digitally sign code and/or files using the public key and private key that correspond to the appropriate level. An individual who possesses the Key from the Metldr area of the system can decrypt and reverse-engineer the Keys for the various levels, which can then be used to sign and encrypt code for those levels of the PS3 System.

13. The PS3 System's access control and encryption TPMs prevent, restrict or otherwise limit access to certain sections of the PS3 System software and hardware. In this way, the TPMs ensure that the PS3 System functions in a safe and reliable manner. They also protect the encrypted firmware, encrypted digital signature Keys and other keys that are stored within the PS3 System. Because the PS3 System and its code are protected by these TPMs, users can neither access nor read the signatures or the Keys, and therefore cannot use those elements to gain access to the System to run a pirated video game.

14. The TPMs described above effectively ensure that video games cannot be copied either to the PS3 System's hard drive or to an external drive and thereafter be accessed or played by a user. If these TPMs are circumvented or disabled, users may be able to copy borrowed (or rented) video game discs, and play those copied video games later without inserting the authentic, licensed disc.

C. Defendants' Circumvention Devices

15. Since the release of the PS3 System, software pirates have attempted to write code to run unauthorized software on SCEA's gaming system. Until recently, their efforts were largely thwarted by the TPMs that secure the various levels of the PS3 System.

16. During their presentation at the 27th annual Chaos Communication Conference, the FAIL0VERFLOW Defendants provided instructions for a method of circumventing the TPMs for certain levels of the PS3 System. By circumventing the PS3 System's TPMs, the FAIL0VERFLOW Defendants were able to discover the private Keys and public Keys that SCEA uses to "digitally sign" all code authorized to run on certain secure levels of the PS3 System.

17. With the FAIL0VERFLOW circumvention instructions, other hackers have circumvented the TPMs and published and trafficked in the private Keys and public Keys corresponding to certain levels of the PS3 System on the Internet.

18. After their presentation at the 27th annual Chaos Communication Conference, the FAIL0VERFLOW Defendants distributed code and software tools derived from their circumvention of the PS3 System's TPMs. The code and software tools can be used as circumvention devices themselves, because they allow users to decrypt, bypass, and/or deactivate the PS3 System's TPMs that would otherwise prevent a user from running unauthorized or unlicensed code.

19. The FAIL0VERFLOW Defendants built upon and could not have developed their circumvention method without information that Hotz derived from his early 2010 attempts to circumvent the TPMs of the PS3 System.

20. In early 2011, after learning of the circumvention methods developed by the FAIL0VERFLOW Defendants, Defendant Hotz circumvented TPMs in the PS3 System to gain access to the Metldr area of the system, and then determine and publish critical Keys to the PS3 System. By publishing those "Metldr keys," Hotz enabled creation of unauthorized firmware that disables TPMs in the PS3 System and will run unauthorized code including illegally copied or modified versions of games. By publishing his "3.55 Firmware Jailbreak" program, Hotz paved the way for video game piracy.

21. In addition to publishing critical keys to the PS3 System, Hotz has also publicly released a series of software programs or tools designed to facilitate and taken advantage of the circumvention of the TPMs in the PS3 System. These programs or tools include the

"dePKG Firmware Decrypter" program, the "3.55 Firmware Jailbreak" program, and the "Signing Tools" program.

22. The purpose of Hotz's "dePKG Firmware Decrypter" program is to decrypt the SCEA firmware necessary to operate the PS3 System. Once decrypted, it is possible for a user to modify the firmware code to disable, avoid, bypass, remove, deactivate and/or impair TPMs in the firmware.

23. Hotz built his "3.55 Firmware Jailbreak" using the Metldr Keys to re-encrypt and re-sign the files decrypted by his "dePKG Firmware Decrypter" program, in order to create and run an unauthorized modified version of SCEA's firmware that circumvents TPMs in the PS3 System.

24. Individuals who implement and/or run Hotz's "3.55 Firmware Jailbreak" program circumvent the TPMs in the PS3 System by disabling, avoiding, bypassing, removing, deactivating and/or impairing a critical TPM in the PS3 System. The "3.55 Firmware Jailbreak" allows users to install and run unauthorized software in circumvention of the TPMs on the PS3 System.

25. Hotz's "Signing Tools" program encrypts and signs unauthorized content so that it will pass scrutiny and run under firmware that is modified to circumvent certain TPMs on the PS3 System, including firmware modified by Hotz's "3.55 Firmware Jailbreak".

26. Hotz utilized, relied upon, and could not have obtained the Keys used to sign code running in the Metldr area without information supplied by the FAIL0VERFLOW Defendants.

27. Based on my examination of the circumvention measures discussed herein, I am convinced that Defendants' devices were designed with the primary purpose and function of circumventing the TPMs in the PS3 System.

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

DATED: January 10, 2011

Bret Mogilefsky