Statement of Andrew "bunnie" Huang, PhD
June 29, 2012

1. As I mentioned in my comments to the Copyright Office in support of proposed classes 3, 4, and 5, "the DMCA makes it risky to engage in basic console repairs that require jailbreaks, such as replacing a worn-out hard drive."[1] This statement is intended to provide more explanation about the situations and circumstances in which video game console repair may require an act of circumvention.

2. Video game console hardware consists of multiple subcomponents. Manufacturers often assign electronic IDs to certain system subcomponents, including hard drives, optical disk drives, and peripherals such as game controllers and memory cards. Unfortunately, these are all items subject to frequent wear-out, loss, and/or routine damage.

3. Secured consoles often verify the electronic ID as part of the measurements made to determine whether the system has been hacked. In practice, electronic IDs can range from a simple serial number to a cryptographic handshake implemented with tamper-resistant modules. Modifying or tampering with the ID in any way typically results in the user being locked out of the console.

4. Replacing a worn-out, lost or damaged component requires bypassing the ID check to prevent the user from being locked out of his or her console. Since the ID check is performed by the secured operating system within the console, bypassing the ID check often requires or involves jailbreaking parts of the system. This is true even if the ID is merely a serial number, as the "original" serial number is remembered by the secured operating system, and bypassing or recovering this record requires a jailbreak.

5. Here are some specific examples of common repairs and replacements that may require acts of circumvention.

    - The original Xbox locks each hard drive to the system with a unique number. When the hard drive wears out, a user must either access and duplicate the ID into a new drive, or if the hard drive is completely broken and the ID inaccessible, a user must jailbreak the system and patch it to allow for a new ID. See http://www.xbox-scene.com/articles/no-modchip-hdd-swap.php for an example of cloning an ID from a drive that is still readable. This technique does not require a modchip, but instead uses the "007" gamesave exploit (which jailbreaks the console) to recover the ID.

[1] *See* http://www.copyright.gov/1201/2012/comments/Andrew_Huang.pdf.

- The Xbox 360 also locks each DVD drive to the system. Replacing the drive requires a jailbreak-enabled analysis of the firmware on the DVD drive to clone the ID information.[2]

- To the best of my understanding, the PS3 also locks its optical drive to the motherboard. Due to a lack of an effective jailbreak at the moment to enable repairs, I believe users have resorted to buying a new DVD drive, pulling the logic board out of the old DVD drive, and putting it into the new DVD drive. This repair operation works because the part that typically wears out is the mechanical assembly, but the crypto-ID is in the logic board. Fortunately, the structure of the DVD drive is amenable to logic board swapping. If the failure is due to a bad logic board, however, I believe the owner is out of luck.

- The Xbox 360 cryptographically identifies peripherals such as game controllers. Therefore, a broken game controller cannot be repaired beyond tape-and-glue or Frankenstein operations. Thus, in most cases, the only practical solution to "fix" a broken game controller is to buy a new one from Microsoft. If jailbreaking either the console or the crypto-ID inside the game controller were to be exempted, that could clear the way for individuals and companies to develop methods for properly repairing and replacing broken game peripherals. From a practical standpoint, it may be easier to jailbreak the game controller's authentication sub-component rather than the console itself, because of the very high security of the console and the policy of banning users from participating in online services when a jailbreak is detected.

[2] *See* http://hardandsoftgaming.wordpress.com/2011/03/12/replacing-a-faulty-xbox-360-dvd-drive-firmware-flash-or-circuit-board-transplant/.