Long Comment Regarding a Proposed Exemption Under 17 U.S.C. 1201

Item 1. Commenter Information

Mike Battilana
m@cloanto.com

Item 2. Proposed Class Addressed

This comment addresses matters shared in large part between, and a possible merger of, two proposed classes:

- 23: Abandoned software – video games requiring server communication
- 24: Abandoned software – music recording software

As such, this same document is being submitted twice (once for each class).

Item 3. Overview

This comment, written from the dual perspective of a software developer and retrocomputing preservationist, supports the circumvention activity sought to be exempted under both classes 23 and 24, but considers the boundaries drawn by the proposed class definitions to be too narrow. Some specific examples are provided as test cases for possible evolutions of the wording.

This comment further aims to address the fact that petition 26 by Richard Kelley and petition 30 by James McCloskey appeared to aim towards a broader definition that could potentially encompass both the proposed classes 23 and 24:

- Richard Kelley's petition 26 defined the proposed classes of works as "Obsolete software/hardware combinations protected by a software based copy protection mechanism (software dongle)";
- James McCloskey's petition 30 included a direct proposal of broadening a previous exemption, namely "Computer programs protected by dongles that prevent access due to malfunction or damage and which are obsolete".

In light of the above, this comment proposes to merge the proposed classes 23 and 24 into one new class, which could be described as:

Software – abandoned TPMs
Computer programs protected by TPMs that prevent access due to malfunction or obsolescence of a required part, and where support for those TPMs has ended. A required part shall be considered obsolete if it is no longer manufactured or if a replacement or repair is no longer reasonably available in the commercial marketplace.

Item 4. Technological Protection Measure(s) and Method(s) of Circumvention

The following TPMs were considered:

- Authentication or matchmaking servers as described in petition 15 by the Electronic Frontier Foundation and Kendra Albert;
- The PACE content protection system as detailed in Richard Kelley's petition 26, in James McCloskey's petition 30, and in Michael Yanoska's petition 44;
- Additional mechanisms described below (which were referenced in the above, but possibly lacked a required factual level of detail).

Before describing additional TPMs, the following comments aim to provide a better understanding of the TPMs as in the already proposed classes 23 and 24:

- Authentication servers are employed by software in general, not only by gaming software. Applications that require communication with a server include well-known productivity applications by Microsoft Corporation, Adobe Systems Incorporated, and numerous other publishers. There is a marketplace of ready-made software components used by software developers of any size to connect to authentication servers without needing to write their own code. As these implementations become more pervasive, almost omnipresent, specificity becomes increasingly difficult to document.
- Authentication servers may stop functioning not only because developer support for those server communications has ended, or because the software was abandoned by the developer (or publisher, or other agent). For example, an internet domain used to connect to the authentication servers may be lost after an inadvertent lack of renewal leads to registration by an unrelated party. The developer may even be willing to remedy the situation, however lack of source code or development tools to modify the old code may make it necessary to resort to "circumvention" of the originally implemented mechanisms in order to continue to use the legitimately acquired software.

Additional TPMs that are directly or indirectly related to the proposed classes and to the underlying petitions:

- Dongles, which were discussed in great length in previous rulemaking processes, and which helped define TPMs in general not only in terms of obsolescence, but also in terms of actual loss of access due to damage or malfunction. In order to satisfy a *de novo* consideration of exemptions, this comment would like to stress how technological evolution is increasing the need to circumvent a growing number of dongle types, specifically because many types of computer ports that were used to connect dongles are disappearing due to being replaced by other, newer but incompatible connectors, and for space reasons, as desktop computers are replaced by notebooks, tablets and smartphones, and many connectors cannot be attached or retrofitted. For example, the next three years are expected to see the new, small and reversible USB "Type C" connector become pervasive across devices. While a simple adapter should allow "legacy" USB dongles to be attached to the new interface, ISA slot dongles cannot be attached outside of a computer, and parallel port dongles are increasingly failing due to lack of driver compatibility on modern 64-bit operating systems. Not to mention older systems like the Commodore PET/CBM, 64 and Amiga computers, which also employed a variety of

dongles (attached to the cassette port, to the mouse/joystick port, and to other expansion and I/O ports). Retrocomputing is a growing trend, and thousands of software titles exist for these "classic" systems, which systems can be emulated on modern hardware, and which software titles may be legitimately purchased or downloaded from preservation sites, but for which increasing harm is caused by the legal uncertainty surrounding emulating a dongle (like the WinUAE emulation software can do) or circumventing the need for a dongle (like "cracked" versions of software do). This harm is increasing, as interest in "retro gaming" is growing (also due to better emulation made possible by more powerful hardware, which follows Moore's Law), while the hardware gap between legacy dongle interfaces and modern devices is widening. In these cases, even if a dongle is not broken per se, it may not be possible to connect it to modern, functioning hardware.

- The function of a "dongle" is sometimes provided by expansion cartridges or peripheral cards which may also serve purposes other than as a pure TPM. For example, the Opal Paint software for the Amiga required the OpalVision graphics card as a TPM mechanism (the software otherwise worked well also without the hardware). Similarly, some versions of the Lightwave software for the Amiga used the Video Toaster expansion board as a TPM (again, the software otherwise worked well also without said board).
- Physical magnetic (floppy, tape) or optical media (CD, DVD) can be specially prepared by using dedicated replication hardware, normally not available to the software or computer user, to write magnetic or optical signals in a way that can be used as a TPM mechanism by software applications. Yet, even without considering the urgency induced by the decay of the media, the 2009-2011 timeframe saw the ending of the production of both floppy disk drives (with Sony Corporation being the last known manufacturer) and DD 3.5" floppy disks. Computer manufacturers have not been using floppy drives for more than 10 years, and "new old stock" is increasingly difficult to find. Optical drives seem to be following a similar trend, last but not least because of the larger form factor. This is causing an increased need for the "protected" media to be converted in a way that either preserves or circumvents the TPM mechanisms. Even when the mechanisms are preserved at the media image level, they are *de facto* circumvented by means of software emulation.

Disabling or bypassing of the TPMs may occur in several ways, including:

- Removal or modification of the software code relating to the implementation of the TPM (e.g. code that verifies for the presence of a dongle or other hardware device or magnetic or optical media characteristics);
- Emulation of the TPM (i.e. creation of a synthetic device or medium which satisfies the requirements of the TPM-protected software), whereby the TPM code does not need to be removed or modified, but the ultimate result is that the original TPM is bypassed;
- Emulation of an authentication server.

Item 5. Asserted Noninfringing Use(s)

In as far as this comment relates to and is focused on computer software, which it does, it draws on previous rulemaking processes and discussions that led to repeat confirmations of the

exemptions for dongles, in similar scenarios. Where a magnetic or optical drive is no longer manufactured, or a computer interface is no longer available or no longer supported by modern operating systems, or an authentication or activation server becomes unavailable, the resulting obsolescence and loss of access due to malfunction or damage of a required part is the same as the one resulting from the loss of access to a "dongle".

This comment proposes a shift of perspective from "Abandoned Software" to software with "Abandoned TPM" which retains a limited scope to a proven narrow and focused subset of copyrighted works.

As discussed here, increasing computing performance, decreasing form factors, and the emerging obsolescence of TPM technologies that were not common in early computer environments, but which gained popularity in the systems that now increasingly need to be preserved (and can be both imaged and emulated well) seems to be causing an increasing burden for comment submission, as thousands of titles would require providing specific, factual support, combined with a *de novo* requirement that does not seem to take into account the unidirectional obsolescence of TPMs.

Additional considerations:

- Legal uncertainty does not affect only end users who "lawfully acquired" a piece of software, or researchers, archivists or libraries. Under a literal interpretation test, developers, publishers and online service providers may be affected too. Example: a preservation site (e.g. hosting 8-bit software from the 1980s) receives a game purported to be uploaded by its original author, with the TPM removed with the help of a third party.
- As projects and organizations increase in complexity, and developers change workplaces, loss of source code is a far more common scenario that might be expected.
- Loss of ability to edit the original source code is also a common scenario. For example, since the 2005 version Microsoft's Visual Studio development environment dropped the ability to create or modify software for systems older than Windows XP.

Item 6. Asserted Adverse Effects

The proposed definition was carefully written in an attempt to avoid adverse effects.

Further clarification on the legal aspects of emulation may be helpful. Increasingly, "everything can be emulated": "copy-protected" media can be imaged reliably, and TPM mechanisms can be emulated. Where does "circumvention" begin?