Petition for Proposed Exemption Under 17 U.S.C. § 1201

Note: This is a Word document that allows users to type into the spaces below.
Please submit a separate petition for each proposed exemption

Item 1. Submitter and Contact Information

Clearly identify the submitter, and, if desired, provide a means for others to contact the submitter or an authorized representative of the submitter by email and/or telephone. (Parties should keep in mind that any private, confidential, or personally identifiable information appearing in this petition will be accessible to the public.)

Submitter: Competitive Carriers Association ("CCA")

CCA is the nation's leading association for competitive wireless providers and stakeholders across the United States. CCA's membership includes more than 100 competitive wireless providers ranging from small, rural carriers serving fewer than 5,000 customers to regional and national providers serving millions of customers. The licensed service area of CCA's carrier members covers more than 95 percent of the nation. CCA also represents approximately 200 associate members consisting of small businesses, vendors, and suppliers that serve carriers of all sizes.

Contact: Rebecca Murphy Thompson, General Counsel
Email: rebecca.thompson@competitivecarriers.org
Telephone: (800) 722-1872

Item 2. Brief Overview of Proposed Exemption

Provide a brief statement describing the proposed exemption (ideally in one to three sentences), explaining the type of copyrighted work involved, the technological protection measure ("TPM") (or access control) sought to be circumvented, and any limitations or conditions that would apply (*e.g.*, a limitation to certain types of users or a requirement that the circumvention be for a certain purpose).

CCA proposes an exemption for connected wearables and consumer machines, often broadly called the "Internet of Things."[1] The connected wearables and consumer machines category consists of a broad category of consumer devices that encompasses the Internet of Things, including connected wearable technologies, such as smartwatches and health monitoring devices, smart meters, connected appliances, connected precision-guided commercial equipment, among others. The specific exemption proposed is as follows:

[1] CCA is filing four separate petitions addressing the following categories: (i) wireless handsets; (ii) all-purpose tablet computers; (iii) mobile hotspots and MiFi devices; and (iv) connected wearables and consumer machines (the Internet of Things). For consistency and efficiency; however, CCA believes that these petitions, and other similar petitions, should be consolidated into a single "wireless device" proceeding, as they all involve computer programs used in devices that connect to a telecommunications and/or broadband network. Consumers do not distinguish among categories of connected devices, and having an exemption only applicable to a subset of wireless devices is likely to cause consumer confusion and frustration.

Computer programs, in the form of firmware or software, or data used by firmware or software, that enable connected wearables and consumer machines to connect to a wireless network that offers telecommunications and/or information services, when circumvention is initiated by the owner of the device, or by another person at the direction of the owner of the device, in order to connect to a wireless network that offers telecommunications and/or information services, and access to the network is authorized by the operator of the network.

Item 3. Copyrighted Works Sought to be Accessed

Identify the specific class, or category, of copyrighted works that the proponent wishes to access through circumvention. The works should reference a category of work referred to in section 102 of title 17 (*e.g.*, literary works, audiovisual works, etc.). Unless the submitter seeks an exemption for the entire category in section 102, the description of works should be further refined to identify the particular subset of work to be subject to the exemption (e.g., e-books, computer programs, motion pictures) and, if applicable, by reference to the medium or device on which the works reside (*e.g.*, motion pictures distributed on DVD).

CCA proposes that consumers should have access through circumvention to a subcategory of copyrighted works identified in 17 U.S.C. Section 102(a)(1): "literary works." The specific subcategory is: "Computer programs, in the form of firmware or software, or data used by firmware or software, that enable connected wearables and consumer machines to connect to a wireless network that offers telecommunications and/or information services."

In House Report No. 94-1476, Congress made it clear that the Section 102(a) copyright category "literary works" includes computer programs: "The term 'literary works' . . . also includes . . . programs to the extent that they incorporate authorship in the programmer's expression of original ideas, as distinguished from the ideas themselves."[2] The firmware and software, and data used by firmware and software contained on connected wearables and consumer machines constitute the expression of original ideas, and not merely the ideas themselves.

Accordingly, the proposed copyright work falls within a well-settled category of copyrighted works, as defined in Section 102 of Title 17.

Item 4. Technological Protection Measure

Describe the TPM that controls access to the work. The petition does not need to describe the specific technical details of the access control measure, but should provide sufficient information to allow the Office to understand the basic nature of the technological measure and why it prevents open access to the work (*e.g.*, the encryption of motion pictures on DVD using the Content Scramble System or the cryptographic authentication protocol on a garage door opener).

[2] H.R. Rep. No. 94-1476 at 54.

CCA proposes to circumvent software or firmware locks on connected wearables and consumer machines that prevent the device from accessing the wireless network of the wireless device owner's choosing.

Connected wearables and consumer machines are hardware or software-locked using a using a variety of methods, including service provider code (SPC) locking, system operator code (SOC) locking, band order locking and Subscriber Identity Module (SIM) locking or Universal Integrated Circuit Card (UICC) locking. These locking mechanisms bind the device to specific wireless networks and prevent consumers from accessing the wireless network of their choice. Only by circumventing these various TPMs can a device owner transfer the use of the device to a network and provider of their choosing.

Item 5. Noninfringing Uses.

Identify the specific noninfringing uses of copyrighted works sought to be facilitated by circumvention (*e.g.*, enabling accessibility for disabled users, copying a lawfully owned computer program for archival purposes, etc.), and the legal (statutory or doctrinal) basis or bases that support the view that the uses are or are likely noninfringing (*e.g.*, because it is a fair use under section 107, it is a permissible use under section 117). Include a brief explanation of how, and by whom, the works will be used.

Consumers who unlock wireless devices such as connected wearables and consumer machines may engage in one or more of several noninfringing uses of the copyrighted software or firmware that resides on their wireless device and permits it to connect to networks. Typically, the circumvention of the TPM allows an owner, who has fulfilled all obligations to the original provider, to operate the device on the network of a new, compatible wireless provider of their choosing. However, certain devices may also unlocked by charitable organizations, who re-sell them to finance charitable works, or by environmental organizations who encourage the re-use of devices to keep toxic chemicals out of landfills.

Noninfringing use of these devices is supported under multiple legal theories, three of which are explained here. First, device unlocking constitutes "fair use" under 17 U.S.C. Section 107. As an initial matter, when most wireless devices are unlocked, the device owner is simply changing the variables in certain memory locations and updating the preferred roaming list (PRL) to make the device useable on the new network. Carriers regularly update the PRL on their customers' devices, so the original author of the copyrighted work intended these variables to be changed without constituting a copyright violation.

Further, unlocking a wireless device meets all four factors of the "fair use" test set forth in Section 107: (1) the purpose of the use is to allow the lawful owner of the device to connect to a wireless network of his or her choice, a reasonable and noninfringing use; (2) the copyrighted work is intended to be changed in this manner and is necessary for the device owner to derive any continued value from the copyrighted work; (3) the amount of the code used in an altered state is extremely small compared to the device operating system as a whole; and (4) the market for and value of the copyrighted work actually increases, as it allows the device to be transferred on the secondary market more easily and to a broader array of buyers.

Second, unlocking a wireless device does not create an infringing "derivative work." This is because, in most instances, unlocking a wireless device does not change the underlying mobile wireless device software, but rather it merely changes underlying variables accessed by the program. As discussed above, these variables are intended by the software designer to be changed, and their change, therefore, does not create an infringing derivative work. Instead, the software is merely being operated by the device owners as intended.

Third, if a derivative work is, in fact, created, it falls within the exception set forth in 17 U.S.C. Section 117(a)(1). This subsection states that a derivative work may be created by the owner of a copyrighted work if the "new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner." Since the changes being made to the copyright work are the same ones that need to be made by the underlying carrier in order for the device to operate properly on its wireless network, such adaptations are inherently "essential step[s] in the utilization of the computer program in conjunction with [the device]." Indeed, in 2012, the Register agreed that unlocking was an "essential step" in the utilization of the device, finding again that "[m]odifications to the firmware or software on the phone may be necessary to make the device functional with another service and better serve the legitimate needs of the consumer."[3]

Item 6. Adverse Effects.

Explain how the inability to circumvent the TPM has or is likely to have adverse effects on the proposed noninfringing uses (*e.g.*, the TPM limits wireless connection to the network of the mobile carrier from which the cellphone was originally purchased or prevents an electronic book from being accessed by screen reading software for the blind). The description should include a brief explanation of the negative impact on uses of copyrighted works. The adverse effects can be current, or may be adverse effects that are likely to occur during the next three years, or both. While the petition must clearly and specifically identify the adverse effects of the TPM, it need not provide a full evidentiary basis for that claim.

The Internet of Things, which includes devices such as wearable consumer products, appliances, in-home connected devices and smart meters, represents the next step in the evolution of the Internet by allowing objects to communicate with other objects. A recent Senate letter estimated that the Internet of Things is expected "to generate global revenues of $8.9 trillion – with over 200 billion connected objects – by 2020."[4]

Unfortunately for consumers, due to a potential inability to choose their desired carrier, their ability to participate in the Internet of Things may be significantly curtailed. Based on reports from CCA members, carriers already are locking consumer machines to specific networks. Indeed, AT&T's unlocking materials from 2014 indicates that it "locks all devices, as

[3] *2012 Recommendation* at 93.

[4] Letter dated October 20, 2014 from Deb Fischer, Cory A. Booker, Kelly Ayotte and Brian Schatz, U.S. Senators to The Honorable Jay Rockefeller, Chairman, U.S. Senate Committee on Commerce, Science & Transportation and The Honorable John Thune, Ranking Member, U.S. Senate Committee on Commerce, Science & Transportation, at 1 ("*Internet of Things Letter*").

of November 11, 2004,"[5] a policy which presumably includes all devices within the Internet of Things.

Critically, the "voluntary" agreement to unlock certain wireless devices *does not include* the Internet of Things, but instead only "phones and tablets . . . that are locked by or at the direction of the carrier."[6] While carriers may provide unlock codes at their own discretion, there is presently nothing preventing them from refusing to unlock these important devices. This lack of commitment presents a significant problem for consumers.

With the "Unlocking Consumer Choice and Wireless Competition Act," Congress instructed the Copyright Office to initiate a rulemaking as to whether "any other category of wireless devices in addition to wireless telephone handsets" should be included within the exemption.[7] It is precisely this type of device – currently locked to a network, and not covered by any carrier voluntary commitment – that the Copyright Office should carefully scrutinize under this directive. Indeed, in addition to this recent Act, members of the Senate Commerce Committee have expressed a desire to tackle the difficult questions posed by the Internet of Things, so that it can "explore how best to preserve America's global leadership position in innovation and economic growth."[8] Part of the Commerce Committee's interest will, no doubt, focus on ensuring that all consumers have equal access to the Internet of Things, something that cannot be accomplished without the Copyright Office's important work.

Absent an anti-circumvention exemption, owners of connected devices will have no right at all to unlock these devices in order to switch carriers or connect to new networks while travelling abroad, rendering them captive to their original carrier. CCA urges the Copyright Office to remedy this anti-consumer circumstance and adopt CCA's proposed exemption in order to allow all consumers to participate in the Internet of Things revolution.

---

[5] *See* http://www.att.com/media/att/2014/support/pdf/ATTMobilityDeviceUnlockCodeInstructions.pdf.
[6] CTIA Consumer Code for Wireless Service, Section 12, *available at* http://www.ctia.org/policy-initiatives/voluntary-guidelines/consumer-code-for-wireless-service.
[7] S 517/PL 113-144, Section 2(b).
[8] *Internet of Things Letter* at 1.