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

[ ] Check here if multimedia evidence is being provided in connection with this comment

Please note that such evidence must be separately submitted on a disc or flash drive. See the Notice of Proposed Rulemaking for detailed instructions.

Item 1. Commenter Information

Identify the commenting party and, if desired, provide a means for others to contact the commenter or an authorized representative of the commenter by email and/or telephone. (Please keep in mind that any private, confidential, or personally identifiable information in this document will be accessible to the public.)

Commenting Party: 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
C. Sean Spivey, Assistant General Counsel
Email: sean.spivey@competitivecarriers.org
Telephone: (800) 722-1872

Item 2. Proposed Class Addressed

Identify the proposed exemption that your comment addresses by the number and name of the class set forth in the Notice of Proposed Rulemaking (e.g., "Proposed Class 7: Audiovisual works – derivative uses – noncommercial remix videos").

Proposed Class 14: Unlocking—Wearable Computing Devices.[1] As noted in the *NPRM*, these devices encompass "wearable mobile wireless devices, a broad category that would include smart watches, fitness devices, health monitoring devices, and perhaps devices such as

[1] CCA originally sought four separate exemptions 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 reiterates its request that these exemptions, and other similar exemptions, should be consolidated into a single "wireless device" exemption, 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.

Google Glass."[2] For simplicity, these devices will be referred to throughout these comments as "wearable devices."

CCA has proposed the following exemption for Proposed Class 14:[3]

> Computer programs, in the form of firmware or software, or data used by firmware or software, that enable connected wearables . . . 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.

CCA believes that this exemption properly enables users to take control over the use of their wearable devices, and permits them the choice of which network they will be connected to. Rather than relying on the presumed goodwill of wireless carriers and the availability of unlocking codes from manufacturers, with this exemption consumers will be empowered to retain their current wearable devices when selecting the wireless service provider of their choice.

Given the growing importance of data as a form of wireless communication among consumers, CCA believes that the most appropriate exemption language is for devices that connect to "telecommunications and/or information services." At present, very few wireless providers offer significant numbers of voice-only plans, and the ever-increasing demand by consumers for data weighs in favor of the Copyright Office clarifying the exemption in this proceeding to confirm that consumers have the right to unlock their devices for the purpose of connecting to wireless networks for both telecommunications and information service uses.

Item 3. Overview

Provide a brief summary of the circumvention activity sought to be exempted or opposed and why.

CCA proposes to circumvent software or firmware locks on a wearable device that prevent the wearable device from accessing the wireless network of the owner's choosing.

The exemption is being sought because wearable device owners have a clear ownership interest in the wearable device itself, as well as the underlying operating system software, and should be afforded the ability to make non-infringing uses of these products. Absent an exemption, wearable device owners may be forced to purchase a new wireless device in order to change service providers and connect to the wireless network of their choice. This may result in substantial and unnecessary costs to the consumer.

---

[2] *Exemption to Prohibition of Circumvention of Copyright Protection Systems for Access Control Technologies*, Notice of Proposed Rulemaking, Docket No. 2014-07, 79 FR 73856, 73865-66 (Dec. 12, 2014) ("*NPRM*").

[3] *NPRM* at 73866, fn. 53; *see also* CCA Consumer Machines Unlocking Pet. at 1-2.

CCA's proposed exemption is not only consistent with the Copyright Office's mandate to allow circumvention where the public interest is served by permitting non-infringing use of the copyrighted material, but also will promote competition and consumer choice in an increasingly consolidated wireless industry.[4]

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

Describe the TPM(s) that control access to the work and the relevant method(s) of circumvention. The description should provide sufficient information to allow the Office to understand the nature of the relevant technologies, as well as how they are disabled or bypassed.

While the Copyright Office is correct that "most smart watches, and most if not all fitness and health monitoring devices, do not employ mobile telecommunications or data networks (e.g., HSPA+ or LTE networks) for wireless connections, but instead use either Wi-Fi to connect to a local wireless network, or Bluetooth or ANT technologies to connect to a smartphone or computer,"[5] CCA believes that "in the next three years [such devices] are likely to be, adversely affected by the prohibition on circumvention"[6] of software locks on such devices.

As batteries and radio transmitters become ever-smaller, it is highly likely that in the very near term such devices will no longer be dependent on Wi-Fi or smartphones for their data connections. Instead, such devices will have their own mobile data connection and be part of the broader array of connected devices. Indeed, this has already begun, as the Google Glass boasts an independent data connection, without reliance on other sources.[7] Similarly, the Smartwatch Group recognizes that "[w]ireless connection to the Internet is done in different ways . . . a smartwatch can also be connected directly to the Internet (usually via integrated mobile phone technology). Such smartphone-independent devices are called 'standalone' smartwatches."[8] Indeed, Samsung has already released the Samsung Gear S, its first network-connected

---

[4] The Federal Communications Commission's recently-released *Seventeenth Report* on mobile wireless competition found that the Herfindahl-Hirschman Index ("HHI"), a measure of market concentration, averaged 3,027 across the country—more than 20% above the level at which a market is considered "highly concentrated." The HHI numbers for the wireless industry have consistently been on the rise over the last five years or more. *See Annual Report and Analysis of Competitive Market Conditions With Respect to Mobile Wireless, Including Commercial Mobile Services*, Seventeenth Report, WT Docket No. 13-135, DA 14-1862, ¶ 32-33 (rel. Dec. 18, 2014).

[5] *NPRM* at 73866.

[6] *NPRM* at 73857.

[7] *See* Engadget Google Glass review, *available at* http://www.engadget.com/products/google/glass/.

[8] Smartwatch Group, "What is a Smartwatch? Definition," *available at* http://www.smartwatchgroup.com/blog/2013/10/28/what-is-a-smartwatch-definition/.

smartwatch that can be used as a standalone mobile device with its own data connection.[9] Once this transition to standalone wearables occurs, there is every expectation that these devices will be locked, as are other mobile wireless devices.

Wearable devices can be hardware or software-locked using a using a variety of methods, including service provider code locking, system operator code locking, band order locking and Subscriber Identity Module locking or Universal Integrated Circuit Card locking. These locking mechanisms would bind the device to specific wireless networks and prevent consumers from accessing the wireless network of their choice. Only by circumventing these various TPMs could a wearable device owner transfer the use of the wearable device to a network and provider of one's choosing.

Wearable devices could be unlocked using a variety of methods currently used to unlock other devices, typically by changing the variables in certain memory locations and updating the preferred roaming list ("PRL") to make the wearable device compatible with a new network. These variables would effectively be a "blank slate" when the wearable device comes off the assembly line, and then updated to make them compatible with the network with which the wearable device is intended to be used. Thus, these variables are and would be intended by the copyright owner to be changed based on which network a particular wearable device will be connected to. In this respect, no unusual or unexpected alterations are being made to the underlying operating system code – instead, anticipated changes are being made that will permit the wearable device to operate.

Item 5. Asserted Noninfringing Use(s)

Explain the asserted noninfringing use(s) of copyrighted works said to be facilitated by the proposed exemption, including all legal (statutory or doctrinal) bases for the claim that the uses are or are likely noninfringing. Commenters should provide an evidentiary basis to support their contentions, including discussion or refutation of specific examples of such uses and, if available, documentary and/or separately submitted multimedia evidence.

Consumers who unlock wearable devices may engage in one or more of several noninfringing uses of the copyrighted software or firmware that resides on their wearable 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 one's choosing. Noninfringing use of these copyrighted works is supported under multiple legal theories, three of which are explained here.

Unlocking Constitutes "Fair Use" Under 17 U.S.C. Section 107

Wearable device unlocking constitutes "fair use" under Section 107 of Title 17 of the United States Code. When most wearable devices are unlocked, the device owner is simply changing the variables in certain memory locations and updating the PRL to make the wearable device useable on the new network. Carriers regularly update the PRL on their customers' wearable devices, so the original author of the copyrighted work intended these variables to be

[9] *See* Samsung Gear S website, *available at* http://www.samsung.com/us/mobile/wearable-tech/SM-R750AZWAATT.

changed without constituting a copyright violation. Further, unlocking a wearable 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 wearable device to connect to a wireless network of their choice, a reasonable and noninfringing use; (2) the copyrighted work is intended to be changed in this manner and is necessary for the wearable 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 wearable device operating system as a whole; and (4) the market for and value of the copyrighted work actually increases, as it allows the wearable device to be transferred on the secondary market more easily and to a broader array of buyers.

Unlocking a Wearable Device Does Not Create an Infringing Derivative Work

Unlocking a wearable device does not create an infringing "derivative work." This is because, in most instances, unlocking a wearable device does not change the underlying wearable 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 wearable device owners as intended.

Any Derivative Work Created is Protected Under 17 U.S.C. Section 117(a)(1)

If, however, 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 copyrighted work are the same ones that need to be made by the underlying carrier in order for the wearable 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 [device] may be necessary to make the device functional with another service and better serve the legitimate needs of the consumer."[10]

Relevant Case Law Demonstrates That Wearable Device Owners are Owners of the Underlying Operating System Software for Section 117(a)(1) Exemption Purposes

In order to fall within the exception set forth in 17 U.S.C. Section 117(a)(1), the party creating the derivative work must also be the owner of the software – that is, if a device owner is a mere licensee of the software, Section 117(a)(1) protections are unavailable to him or her.[11] Although the Supreme Court has not articulated a national framework on this issue, the two

[10] *2012 Recommendation* at 93.

[11] Contrary to the arguments raised by CTIA in the 2012 proceeding, simply stating that a piece of software is being provided under "license" does not make it so. *See Vernor v. Autodesk, Inc.*, 621 F.3d 1102, 1180 (9th Cir. 2010) (holding that simply labeling a software agreement as a license is not "dispositive").

leading cases on licensing vs. ownership are *Krause v. Titleserv, Inc.*, 402 F.3d 119 (2d Cir. 2005) and *Vernor v. Autodesk, Inc.*, 621 F.3d 1102 (9th Cir. 2010). In the *2012 Recommendation*, the Register concluded that the state of the law was sufficiently unclear as to make it impossible to determine whether all device owners were licensees or owners of the software.[12] Despite this determination, the current state of the market and the terms on which much of the operating system software is provided to consumers in connection with a wearable device purchase make it clear that wearable device owners are the also the owners of the operating system software under either the *Krause* or the *Vernor* tests.

In *Krause*, the Second Circuit held that ownership of a copyrighted work, as opposed to license, is indicated by balancing seven factors:

> (1) whether substantial consideration was paid for the copy; (2) whether the copy was created for the sole benefit of the purchaser; (3) whether the copy was customized to serve the purchaser's use; (4) whether the copy was stored on property owned by the purchaser; (5) whether the creator reserved the right to repossess the copy; (6) whether the creator agreed that the purchaser had the right to possess and use the programs forever regardless of whether the relationship between the parties terminated; and (7) whether the purchaser was free to discard or destroy the copy anytime it wished.[13]

With respect to wearable devices, wearable device owners pay substantial consideration for the copy of the software as part of the wearable device price.[14] The copy of the software is stored on property owned, namely the physical wearable device, and the software creator permits the underlying operating system software to be used by the wearable device owner indefinitely (and in some cases, even longer due to transfer rights). Further, the wearable device owner is free to discard or destroy the copy (along with the physical wearable device) anytime that he or she wishes. On balance, these *Krause* factors strongly favor a finding of ownership of the copyrighted operating system software by the wireless device owner.

In *Vernor*, the Ninth Circuit held that "a software user is a licensee rather than an owner of a copy where the copyright owner (1) specifies that the user is granted a license; (2) significantly restricts the user's ability to transfer the software; and (3) imposes notable use restrictions."[15] These factors can be seen as more stringent, and it has been argued by some that they favor the view that the device owner is a licensee. Nevertheless, the test for ownership of a

---

[12] *2012 Recommendation* at 92 ("The Register concludes that the state of the law remains unclear. Although *Vernor* and *Krause* are useful guideposts in considering the status of software ownership, they are controlling precedent in only two circuits and are inconsistent in their approach; whether and how those standards would be applied in other circuits is unknown.")

[13] *Krause*, 402 F.3d at 124.

[14] For example, the price for a Samsung Gear 2 smartwatch is $199, with the hardware components of the wearable device combining to form only a small portion of the cost of the device. *See* http://www.samsung.com/us/mobile/wearable-tech/SM-R3810ZKAXAR.

[15] *Vernor*, 621 F.3d at 1111.

wearable device's underlying operating system is met under the *Vernor* test as well. Importantly, the *Vernor* test is a conjunctive test, and therefore demands that all three elements be met if a software user is to be considered a licensee, rather than an owner.[16]

As applied to the facts at hand, wearable devices do not have "notable use restrictions." Customers are permitted to use their wearable devices for any lawful purpose, and as the Register stated in the *2012 Recommendation*, "no wireless provider has taken the position that customers are unable to sell devices that they no longer use, or transfer them to a spouse, child or friend."[17] Accordingly, wearable device operating system software fails one element of the *Vernor* test, and on this basis alone a court could conclude that an owner of a wearable device is also an owner of the copy of the operating system software.

Given the evidence above, it is clear that wearable device owners should be considered owners of a copy of the operating system software, and therefore entitled to the protections of Section 117(a)(1), and be permitted to create a derivative work in order to allow the wearable device to connect to a wireless network of the wearable device owners choice.

Item 6. Asserted Adverse Effects

Explain whether the inability to circumvent the TPM(s) at issue has or is likely to have adverse effects on the asserted noninfringing use(s), including any relevant legal (statutory or doctrinal) considerations. Commenters should also address any potential alternatives that permit the asserted noninfringing use(s) without the need for circumvention. Commenters should provide an evidentiary basis to support their contentions, including discussion or refutation of specific examples of such uses and, if available, documentary and/or separately submitted multimedia evidence.

The most clear, and most immediate, adverse effect that the TPMs that lock wearable devices have is to prevent consumers from easily switching their wearable devices to the competing network of their choice. Although carriers may unlock under certain circumstances, owners should not be beholden to the carrier after completion of service agreement commitments. As the Senate has noted, there are also "circumstances in which additional avenues for unlocking may be preferable over attempting to unlock through the carrier."[18] Absent an exemption, TPMs used to lock wearable devices to a particular network will foreclose the ability to exercise preferable, and in some cases, the only, avenues to unlock devices. Since circumvention to connect to an alternative network would be a noninfringing use of the copyrighted work, consumers should have the freedom to unlock their wearable devices on their own or through an agent of their choosing.

---

[16] *See* YULE KIM, CONGRESSIONAL RESEARCH SERVICE, STATUTORY INTERPRETATION: GENERAL PRINCIPLES AND RECENT TRENDS, Order Code 97-589 at 8 (updated Aug. 31, 2008) ("Ordinarily, as in everyday English, use of the conjunctive 'and' in a list means that all of the listed requirements must be satisfied . . . .").

[17] *2012 Recommendation* at 92 (*quoting* MetroPCS Comments at 17).

[18] Senate Report 113-212, *available at* http://www.gpo.gov/fdsys/pkg/CRPT-113srpt212/html/CRPT-113srpt212.htm.

Wearable Devices are Not Subject to the Current CTIA "Voluntary" Unlocking Agreement, and Individual Carrier Policies are Insufficient to Protect Consumer Interests

It is clear that carriers are indeed locking wearable devices, and are likely to increasingly do so during the exemption period.[19] AT&T, one of the largest wireless carriers in the nation, makes their locking policy for all devices clear, stating that the company "locks all devices, as of November 11, 2004."[20]

Critically, the CTIA "voluntary" agreement currently in place to unlock certain wireless devices does not include wearable devices, but instead only "phones and tablets . . . that are locked by or at the direction of the carrier."[21] 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.

Even if a carrier were to have a "voluntary" unlocking policy for wearable devices, the exemption would remain necessary. As NTIA noted in the last triennial review, and the voluntary agreement confirms, oftentimes carriers must have the necessary code or the ability to reasonably obtain it to unlock a device.[22] Where a voluntary agreement only requires that a carrier "initiate a request to the [original equipment manufacturer ("OEM")] to unlock the eligible device" it is possible for the carrier to comply with the agreement in a manner that does not ultimately result in the consumer's device being unlocked.

This also highlights the fact that OEMs (or third-party software developers) often consider themselves to be the owners of the copyrighted software, which is provided under a purported license to carriers. So, there remains the possibility an OEM or software developer may refuse to allow carriers to alter their software in any respect, which would eliminate the ability of carriers to implement their voluntary unlocking promises. In such a circumstance, a consumer unlocking exemption granted in this proceeding would be the only path to allowing customers to switch wireless providers with their devices in hand. And, this circumstance is not farfetched or theoretical. Indeed, in a recent discussion of the company's post-sale transition plan, Cincinnati Bell Wireless ("CBW") stated that it would only be allowing customers to

---

[19] Several of the largest carriers are offering the Samsung Gear S "on contract," suggesting the use of TPMs. *See* Michael Rogueau, "Major US carriers reveal Samsung Gear S release date," Techradar (Nov. 7, 2014), *available at* http://www.techradar.com/news/portable-devices/other-devices/the-samsung-gear-s-release-date-is-sometime-this-fall-1266593.

[20] *See* http://www.att.com/media/att/2014/support/pdf/ATTMobilityDeviceUnlockCodeInstructions.pdf .

[21] CTIA Consumer Code for Wireless Service, Section 12, *available at* http://www.ctia.org/policy-initiatives/voluntary-guidelines/consumer-code-for-wireless-service.

[22] NTIA Reply Comments at 16, *available at* http://www.copyright.gov/1201/2012/2012_NTIA_Letter.pdf; CTIA Consumer Code of Conduct § 12.

unlock their handsets to move to another carrier if the handsets were "one year old or newer."[23] Even with this significant restriction, CBW would only permit customers to "transition to another provider by providing unlock codes *(if available)*," suggesting that there are a sufficient number of circumstances in which unlock codes are not available to warrant a specific disclosure.[24] Although this was in the context of wireless handsets, it is not a significant leap to assume that the same is or would be the case for similarly-situated wearable device customers.

Thus there is clear evidence that voluntary unlocking policies do not obviate the need for an exemption. As a result, customers must have the option and the right to unlock their wearable devices to realize their full utility, and without unwarranted interference from their original wireless provider.[25]

The Availability of Unlocked Wearable Device Options Does Not Obviate the Need for an Exemption

Further, the availability of unlocked wearable device options in the marketplace does not displace the need for a wearable device unlocking exemption. Although some, but by no means all, wearable devices are available in an unlocked form, a consumer may not find her desired wearable device as one of the unlocked options. But perhaps more importantly, a consumer may simply wish to keep his current familiar wearable device, or that is, for example, particularly well-suited to their needs. Where owners are unable to unlock their current wearable device to connect to their network of choice, they are effectively forced to purchase a new wearable device, despite having no desire to do so.

Substantial Evidence of Adverse Effects Exists, and Consumers Have No Reasonable Alternatives to Circumvention

After the previous unlocking exemption was allowed to expire, Congress saw sufficient current adverse effects, as well as the potential for adverse effects, to immediately reinstate and expand the exemption in the "Unlocking Consumer Choice and Wireless Competition Act." Even with other voluntary unlocking policies in place, Congress saw sufficient harm in the marketplace to adopt legislation. And, in this respect, Congress was performing the will of the people. A White House petition garnered more than 114,000 signatures from concerned consumers who demonstrated the likely adverse effects of the rejection of the unlocking

[23] Phil Goldstein, "Cincinnati Bell customers frustrated by transition amid network shutdown," FierceWireless (Jan. 12, 2015), *available at* http://www.fiercewireless.com/story/cincinnati-bell-customers-frustrated-transition-amid-network-shutdown/2015-01-12.

[24] *Id.*

[25] CCA notes that the exemption never has, and never should be, held to protect "bulk circumvention." Previous exemptions have specifically excluded bulk resellers from the exemption's protections, and CCA notes that there may be further breach of contract protections and other legal claims that victims of bulk resellers may assert to protect their rights.

exemption.[26] Indeed, this consumer outcry extended not only to the original exemption or wireless handsets, but also to other wireless devices as well. As part of the "Unlocking Consumer Choice and Wireless Competition Act," Congress directed the Copyright Office to expand its inquiry into other wireless devices, such as wearable devices, to ensure that anti-competitive locking policies were not harming the market for these important consumer products as well. Even with voluntary unlocking policies for handsets and tablets already in place, Congress saw sufficient harm in the marketplace to adopt legislation directing the Copyright Office to undertake this new examination.

Additionally, NTIA petitioned the FCC to commence a rulemaking to require carriers to unlock devices upon request.[27] NTIA stated that a rule would "increase competition in the mobile services market and enhance consumer welfare."[28] While the enactment of the Unlocking Consumer Choice and Wireless Competition Act foreclosed the need for rulemaking, not extending an exemption would have the adverse effects of decreased competition and consumer welfare.

No viable alternatives to circumvention have emerged over the last three years, nor is CCA aware of any on the horizon. As a result, the Copyright Office remains consumers' best hope for a continued ability to lawfully unlock their wearable devices. The Copyright Office should heed the outcry from consumers, Congress and the Administration about the current and potential anti-consumer harms that failing to adopt a wearable device unlocking exemption would bring, and adopt CCA's proposed exemption.

Item 7. Statutory Factors

Evaluate the proposed exemption in light of each of the statutory factors set forth in 17 U.S.C. 1201(a)(1)(C):

(i) the availability for use of copyrighted works;

Without question locks on wearable devices reduces the availability for use and usability of the copyrighted software operating system. A customer who would otherwise be technically able to use his or her device on a competing network is prevented from doing so by artificial locks. Thus, the ability to use the copyrighted operating system software that powers the wearable device is substantially limited; if a customer switches networks and has a wearable device that cannot be unlocked, he or she is no longer able to use the copyrighted operating system.

Importantly, as the Register found during the prior proceeding:

---

[26] *See* R. David Edelman, "It's Time to Legalize Cell Phone Unlocking," Official White House Response to Make Unlocking Cell Phones Legal, *available at* https://petitions.whitehouse.gov/response/its-time-legalize-cell-phone-unlocking.

[27] NTIA, Petition for Rulemaking of the National Telecommunications and Information Administration (filed Sept. 17, 2013), *available at* http://www.ntia.doc.gov/files/ntia/publications/ntia_mobile_devices_unlocking_petition_09172013.pdf.

[28] *Id*. at 1.

> There is no indication that mobile . . . firmware is sold in any way other than with the [device] for which it is developed, and no indication that there are alternative "formats" available that would not require circumvention – that is, there is no evidence that users of locked legacy [devices] can simply install an alternative operating system that does not include carrier locks. Accordingly, the first factor favors an exemption.[29]

These facts remain as true today as they did in 2012. CCA is unaware of wearable device firmware being sold in any other way than bundled with the wearable device for which it was developed, and is aware of no other formats of such operating system software available that would not require circumvention. As such, the Register should make the same finding in this proceeding that the first statutory favor favors an exemption.

(ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;

An exemption permitting the unlocking of wearable devices increase the availability of the copyrighted operating system works for use for nonprofit archival, preservation, and educational purposes. As an initial matter, a significant number of nonprofit organizations fund their operations through the collection, unlocking and resale of wireless devices. In addition, artificial locks on wearable device software may prevent those operating systems from being studied in the classroom or archived for future study. An exemption to the prohibition on circumvention of wearable device locks certainly will not negatively impact, and may in fact promote, the use of these works for such purposes.

(iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;

Similar to the use of the works for nonprofit and educational purposes, there should be no concern that a wearable device unlocking exemption will have any negative impact on criticism, comment, news reporting, teaching, scholarship or research. In fact, there may be positive benefits for these fields that flow from an unlocking exemption. For example, journalists can improve consumer awareness by writing about the behavior of an unlocked device moving from one network to another. Similarly, this would allow industry commenters to review the performance of a single wearable device on multiple wireless networks.

(iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and

If anything, the circumvention of wearable device locks actually *improves* the market value of the copyrighted work. Since the operating system conveys with the wireless device, the creator of the copyrighted work is actually benefited by being able to reach the widest possible audience. If a wearable device is locked to a particular network, it inherently has a smaller base of customers on the secondary market, and is therefore worth less to the original purchaser. The operating system is a large part of the value of the fully operational wearable device, and

[29] *2012 Recommendation* at 97.

customers will be willing to pay more for a wearable device (and the underlying operating system) that is worth more, and can be transferred more easily, on the secondary market.

Although the Register found that the market for mobile device operating system software was "unlikely to be affected by enabling consumers to alter that software for the purpose of using the handset on another carrier," this was coupled with the finding that "[t]here is nothing in the record to suggest that the market for firmware has declined in the six years following the first granting of an unlocking exemption."[30] CCA agrees with the Register's prior determination. In fact, the market for firmware (and the wearable devices with which it is sold) has only increased since the Register made that determination in 2012. A recent CTIA survey cited by the Federal Communications Commission found that "the number of connections grew . . . from 326.5 million at the end of 2012, to 335.7 million at the end of 2013 [or 3 percent]."[31] Thus, it can be demonstrated that the market for firmware (and the wireless devices with which it is sold) has only increased since the Register made its determination in 2012. Accordingly, the Register should again draw the same conclusion, based on the same or stronger current evidence, that "the fourth factor . . . favors an exemption."[32]

(v) any other factor that may be appropriate for the Librarian to consider in evaluating the proposed exemption.

The Librarian should consider the positive impact that an unlocking exemption will have on consumer choice and competition in the wireless industry. By allowing customers to have control over their own wireless devices, and to put them on the network of their choosing, the Librarian is conferring a significant social benefit. The Librarian should empower consumers to make informed choices about wireless services.

Item 8. Documentary Evidence

Commenters are encouraged to submit documentary evidence to support their arguments or illustrate pertinent points concerning the proposed exemption. Any such documentary evidence should be attached to the comment and uploaded through the Office's website (though it does not count toward the 25-page limit).

None submitted.

[30] *2012 Recommendation* at 98.

[31] *Seventeenth Report* at ¶ 20 (*citing* CTIA Wireless Industry Indices at 7).

[32] *2012 Recommendation* at 98.