Before the  
U.S. COPYRIGHT OFFICE 
LIBRARY OF CONGRESS 
Washington, DC 20559 

In the Matter of ) 
) 
Exemption to Prohibition on ) Docket No. RM 2011-7 
Circumvention ) 
of Copyright Protection Systems for ) 
Access Control Technologies )

Reply Comments of 

CONSUMERS UNION 

Represented by: 
Laura M. Moy*  
Angela J. Campbell  
Institute for Public Representation  
Georgetown University Law Center  
600 New Jersey Avenue, NW  
Suite 312  
Washington, DC 20001  
(202) 662-9535 

Of counsel: 
Parul P. Desai, Esq.  
Communications Policy Counsel  
Consumers Union 

Dated: March 2, 2012 

* Admitted to the Maryland bar only; DC bar membership pending. Practice supervised by members of the DC bar.
INTRODUCTION & SUMMARY

These reply comments are respectfully submitted on behalf of Consumers Union (“CU”), an independent nonprofit organization whose mission is to work for a fair, just, and safe marketplace for all consumers and to empower consumers to protect themselves. This reply is in support of proposed exemption 6A:

Computer programs, in the form of firmware or software, including data used by those programs, that enable mobile devices to connect to a wireless communications network, when circumvention is initiated by the owner of the device to remove a restriction that limits the device’s operability to a limited number of networks, or circumvention is initiated to connect to a wireless communications network.¹

Parts of this reply also support proposed exemptions 6B and 6C.

CU herein responds to the initial comments filed on behalf of CTIA – The Wireless Association® (“CTIA”) opposing the proposed exemptions 6A, 6B, and 6C.² Contrary to CTIA’s claims, there is substantial support for the DMCA anti-circumvention exemption proposed by Consumers Union. The activity described by the exemption constitutes a noninfringing use that does not infringe on either the reproduction right or the derivative works right of any holder of mobile device firmware or software copyright. Declining to adopt the proposed exemption would have clear adverse effects on the noninfringing use at issue.

¹ Proposal of Consumers Union, RM 2011-7 [hereinafter CU Proposal].
# TABLE OF CONTENTS

**INTRODUCTION & SUMMARY** .........................................................................................................................................................i

I. **Removing a Mobile Device Lock Does Not Violate Any of the Exclusive Rights of Mobile Device Firmware or Software Copyright Holders** ..................1
   A. The Aspect of Mobile Device Computer Programs that Facilitates Connectivity of a Device to a Communications Network May Be Unprotectable Under U.S. Copyright Law ..................................................................................1
   B. Removing a Mobile Device Lock Does Not Create a Derivative Work ...............3
   C. Removing a Mobile Device Lock Does Not Infringe Upon the Reproduction Right .................................................................................................................................................4
   D. Fair Use Analysis Is Not Necessary to Determine that Mobile Device Unlocking Constitutes Noninfringing Use.........................................................................................................................................................6
   E. Mobile Device Unlocking Is A Noninfringing Use Regardless of Who Does It, Whether the Device in Question Is New or Used, Who Owns the Copy of the Computer Program, and What the Motive Is for Unlocking ..................6

II. **Application of the Anti-Circumvention Provision to Mobile Device Unlocking Would Have Clear Adverse Effects** .........................................................................................................................8
   A. Wireless Carriers Are Often Unwilling to Unlock Consumers’ Devices ..........9
   B. The Adverse Effects of Applying the Anti-Circumvention Provision Would Extend to Consumers’ Ability to Engage in Noninfringing Unlocking of “Mobile Devices” ..........................................................................................................................................................12

III. **Conclusion** ..............................................................................................................................................................................13
I. REMOVING A MOBILE DEVICE LOCK DOES NOT VIOLATE ANY OF THE EXCLUSIVE RIGHTS OF MOBILE DEVICE FIRMWARE OR SOFTWARE COPYRIGHT HOLDERS

In their initial proposals, proponents of proposed exemptions 6A, 6B, and 6C presented several theories under which mobile device unlocking constitutes a noninfringing use of mobile device firmware or software. No commenter on the initial proposals has presented an opposing theory to demonstrate why, notwithstanding these theories, unlocking nevertheless infringes one or more of copyright holders’ exclusive rights.

A. The Aspect of Mobile Device Computer Programs that Facilitates Connectivity of a Device to a Communications Network May Be Unprotectable Under U.S. Copyright Law

CTIA points out that “CU offers no evidence that the protected firmware or software is not protected by copyright.” This is because that argument has not been presented. That “firmware or software is a computer program, and . . . computer programs . . . are prima facie copyrightable subject matter” is not in controversy. This observation is not “contrary” to anything in CU’s proposal, as CTIA’s analysis asserts.

CU’s arguments do not challenge Apple v. Franklin. Rather than argue that mobile device firmware is categorically uncopyrightable—an overbroad argument that CU does not endorse—CU has argued that the limited “feature of mobile device firmware or software that facilitates connectivity of a device to a communications network may be unprotectable under U.S.

---

3 CTIA Comments at 30.
4 Id.
5 Id.
6 Id.
7 Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1253 (3d Cir. 1983) (“Franklin’s contentions that operating system programs are per se not copyrightable is unpersuasive.”).
This argument is supported by two well-established principles of copyright law: 1) that “U.S. copyright law pertains only to the expression of intellectual concepts, and not to underlying ideas,” and 2) that because computer programs “typically include elements of both expression and idea in the same body of work . . . within a single [computer] program, it is possible for unprotectable features to coexist with protectable features.”

In the context of an operating system, “the line [between idea and expression] must be a pragmatic one, which also keeps in consideration ‘the preservation of the balance between competition and protection reflected in the patent and copyright laws’.” The focus is “on whether the idea is capable of various modes of expression.” “The question, however, is not whether any alternatives theoretically exist; it is whether other options practically exist under the circumstances.” This is because when, under the circumstances, other options do not practically exist, the merger doctrine precludes copyright protection for those elements in which idea and expression merge.

---

8 CU Proposal at 9.
9 Id. (citing 17 U.S.C. § 102(b) (“In no case does copyright protection . . . extend to any idea, procedure, process, system, method of operation, concept, principle, or discovery, regardless of the form in which it is described, explained illustrated, or embodied in such work.”)).
10 Id. (citing Computer Assocs. Int’l v. Altai, 982 F.2d 693, 705 (2d Cir. 1992) (“those elements of a computer program that are necessarily incidental to its function are . . . unprotectable.”); Sega Enters. v. Accolade, Inc., 977 F.2d 1510, 1525 (9th Cir. 1992) (“Under a test that breaks down a computer program into its component subroutines and sub-subroutines and then identifies the idea or core functional element of each . . . many aspects of the program are not protected by copyright.”); General Universal Sys. v. Lee, 379 F.3d 131, 142 (5th Cir. 2004) (“To assess a claim of software infringement, we have generally endorsed the ‘abstraction-filtration-comparison’ test . . . a three-step procedure to assess whether protectable expression has been improperly copied.”); R.C. Olmstead, Inc. v. CU Interface, LLC, 606 F.3d 262, 272 (6th Cir. 2010) (software developer failed to “identify those elements of the [allegedly infringing] software that are unique and original, rather than necessary to the function of any credit union software.”)).
11 Franklin Computer, 714 F.2d at 1253.
12 Id.
In order to determine whether the merger doctrine precludes copyright protection to an aspect of a program’s structure that is so oriented [toward efficiency], a court must inquire whether the use of this particular set of modules is necessary sufficiently to implement that part of the program’s process being implemented. If the answer is yes, then the expression represented by the programmer’s choice of a specific module or group of modules has merged with their underlying idea and is unprotected.  

As MetroPCS has explained, the aspects of mobile device computer programs that facilitate connectivity to a single or limited number of networks typically comprise mere variables accessed and intended to be used by the software or firmware. Because use of these particular variables is necessary to efficiently implement network connectivity under the circumstances, these variables are not independently copyrightable.

B. Removing a Mobile Device Lock Does Not Create a Derivative Work

To constitute a derivative work, “[a] work consisting of editorial revisions, annotations, elaborations, or other modifications” must “as a whole, represent an original work of authorship.” As MetroPCS explains in its proposal, unlocking or re-flashing a device merely changes the underlying variables that are accessed and intended to be used by the software or firmware. Unlocking or re-flashing therefore only creates a derivative work if the modifications to these variables add up to a work that meets the minimum requirements for copyrightability. As explained above, these variables do not meet those requirements because in the context of a mobile device computer program, uncopyrightable idea merges with copyrightable expression in these variables. Therefore, these variables constitute unprotectable idea rather than protectable expression.

---

17 MetroPCS Proposal at 16.
Even if these mere variables could be considered expression, modifications to these variables would still not meet the minimum requirements for copyrightability central to formation of a derivative work. “[O]riginality is a constitutionally mandated prerequisite for copyright protection.”\(^\text{18}\) Trivial contributions to a prior work are insufficiently original to support a copyright.\(^\text{19}\) For the additional matter injected in a prior work to satisfy originality, that matter must constitute more than a minimal contribution.\(^\text{20}\) Changes to underlying variables accessed and intended to be used by mobile device software or firmware are trivial changes that do not rise to the level of originality necessary to form a derivative work.

C. Removing a Mobile Device Lock Does Not Infringe Upon the Reproduction Right

As MetroPCS has explained, re-flashing a wireless device is a write-only process that entails the writing only of underlying variables, not a substantial portion of the copyrighted program,\(^\text{21}\) thus, re-flashing does not result in a new reproduction of the work.

The only way in which mobile device unlocking might conceivably implicate the copyright holder’s reproduction right is under a theory that has not been raised in this proceeding by opponents of the proposed exemption: that the device user’s license to reproduce the work in the RAM of the device is revoked the instant the user violates her Terms of Service by using the device on another carrier’s network, and because it is impossible to use the device without continuously making reproductions of the work in


\(^{19}\) *L. Batlin & Son, Inc. v. Snyder*, 536 F.2d 486, 487–488 (2d Cir. N.Y. 1976) (finding that trivial differences between appellants’ plastic bank and a cast iron bank in the public domain were insufficiently original to support copyright), *cert. denied*, 429 U.S. 857 (1976).

\(^{20}\) See 1-3 *Nimmer on Copyright* § 3.03 (providing numerous examples of circumstances in which courts have found the additional matter insufficient to satisfy originality).

\(^{21}\) MetroPCS Proposal at 16.
the RAM of the device, any subsequent use of the device therefore infringes the reproduction right.22

Under this theory, a user of a mobile device who has violated her carrier’s Terms of Service would engage in copyright infringement merely by *turning on* the device. In other words, as soon as the customer violates her Terms of Service, she has no choice but to throw her device in the garbage, because she can never turn it on again without subjecting herself to liability under copyright law. As CU has argued, this theory is barred by the misuse doctrine. The theory is likely also barred, as MetroPCS has argued, by the doctrine against equitable servitudes on personal property.23

In response, CTIA claims that “[i]n *Apple, Inc. v. Psystar Corp.*, the closest and most recent [misuse] case cited by CU, Ninth Circuit rejected a defense of copyright misuse against a claim remarkably similar to that made here by CU.”24 But the software licensing agreement at issue in *Psystar* required only “that the Mac OS X be used exclusively on Apple computers.”25 It did not prohibit otherwise lawful activities that one might accomplish using the software preinstalled on Apple computers, conditioning continuing validity of the license on the user’s avoidance of the proscribed activities. The license at issue in *Psystar* would be more closely analogous to that presented by Virgin in the last DMCA proceeding if, in addition to requiring that Mac OS X be used exclusively on Apple computers, it required that Apple computers sold with preinstalled copies of Mac OS X access the internet only via a specific internet service provider (*e.g.*, Comcast or Time Warner).

Notably, in the current DMCA rulemaking no commenter has attempted to demonstrate that a particular software license renders mobile device unlocking an infringement of the reproduction right. CTIA is correct that CU has not “ma[de] any

---

22 This theory was presented in the prior DMCA rulemaking. Reply Comments of Virgin Mobile USA, L.P., RM 2008-8, at 18–19. In anticipation of its possible advancement by opponents in the current proceeding, CU refuted the theory in its proposal. CU Proposal at 10.

23 MetroPCS Proposal at 24.

24 CTIA Comments at 33 (internal citations removed).

25 *Apple Inc. v. Psystar Corp.*, 658 F.3d 1150, 1153 (9th Cir. 2011).
showing that any license of a carrier includes this type of anti-competitive prohibitions in its licenses.”

This is because this type of anti-competitive prohibition would not be enforceable.

There is thus no cognizable theory under which removing a mobile device lock might constitute an infringement of the exclusive reproduction right.

D. Fair Use Analysis Is Not Necessary to Determine that Mobile Device Unlocking Constitutes Noninfringing Use

CTIA correctly observes that “[n]ot one of the Proponents even attempted to justify their proposed unlocking activities as fair use under the Copyright Act.” This is because, as a defense doctrine, fair use is only relevant when the activity at issue, unlike mobile device unlocking, would otherwise constitute infringement. But this rulemaking under section 1201 is concerned with noninfringing uses of copyrighted works in general, not just with fair uses. Unlocking or re-flashing is a noninfringing use of mobile device firmware or software not merely because it is defensible under fair use, but because it does not infringe upon any of the exclusive rights assigned to rightsholders in the first place.

Nevertheless, even if unlocking or re-flashing were somehow found to satisfy a prima facie test for copyright infringement, it would likely be noninfringing under fair use analysis.

E. Mobile Device Unlocking Is A Noninfringing Use Regardless of Who Does It, Whether the Device in Question Is New or Used, Who Owns the Copy of the Computer Program, and What the Motive Is for Unlocking

For the reasons Proponents have advanced, mobile device unlocking constitutes a noninfringing use of mobile device firmware. CTIA argues that an expanded

---

26 CTIA Comments at 34.
27 CTIA Comments at 29.
unlocking exemption should not be granted because it fears that such an exemption would assist bulk resellers and harm wireless carriers’ business.\(^\text{30}\) But as CTIA points out, “Nowhere . . . does the legislative history identify the desire to support the business models of commercial enterprises as a factor animating its decision to relax the section 1201(a)(1) anticircumvention ban by establishing a rulemaking proceeding.”\(^\text{31}\) The legislative history is no more supportive of the business models of wireless carriers than it is of bulk resellers.

The question properly before the Register is whether persons who are users of a copyrighted work are, or are likely to be, adversely affected by the anti-circumvention prohibition in their ability to make noninfringing uses of a particular class of copyrighted works.\(^\text{32}\) Where, like here, the noninfringing nature of the use at issue is not affected by who accomplishes the act of unlocking, how old or used the device in question is, who owns the copy of the computer program, or what the motive is for unlocking, such limitations would unnecessarily limit consumers’ ability to make this obviously valuable noninfringing use of mobile device software and therefore should not be built into the exemption.

Moreover, the DMCA is neither a necessary nor effective vehicle for combating bulk reselling. As CU argued in its proposal, “carriers have prevailed [against bulk resellers] on several types of claims in addition to DMCA claims.”\(^\text{33}\) Nonetheless, as CTIA points out, “[r]ampant subsidy theft continues.”\(^\text{34}\) This is in spite of the fact that “CTIA members continue to spend millions of dollars to combat this activity” on litigation that “has been extremely expensive and has not succeeded in stopping subsidy theft.”\(^\text{35}\)

\(^{30}\) CTIA Comments at 49–50, 57–59.
\(^{31}\) CTIA Comments at 13–14.
\(^{32}\) See 17 U.S.C. § 1201
\(^{33}\) CU Proposal at 25.
\(^{34}\) CTIA Comments at 50.
\(^{35}\) Id.
Finally, CTIA’s assertion that the Copyright Office would “condone illegal access to [wireless] networks” if it approved an unlocking exemption not expressly limited to situations in which “access to the network is authorized” is without merit.\textsuperscript{36} “Illegal access” to wireless networks is already illegal. Nevertheless, CU would not object to the addition of language limiting the exemption to circumstances in which the purpose of circumvention is not an independently illegal activity.

Computer programs, in the form of firmware or software, including data used by those programs, that enable mobile devices to connect to a wireless communications network, when circumvention is initiated by the owner of the device to remove a restriction that limits the device’s operability to a limited number of networks, or circumvention is initiated to connect to a wireless communications network; \textbf{and when circumvention is not initiated for the purpose of engaging in independently illegal activity.}

\section*{II. APPLICATION OF THE ANTI-CIRCUMVENTION PROVISION TO MOBILE DEVICE UNLOCKING WOULD HAVE CLEAR ADVERSE EFFECTS}

CTIA argues that “none of the proponents [of the unlocking exemption] have come remotely close to demonstrating the requisite ‘likely’ adverse impact on noninfringing uses sufficient to justify their requested exemption.”\textsuperscript{37} It is difficult to understand why CTIA believes the adverse effects of not granting this exemption are unclear. If mobile device unlocking—a widespread activity performed by countless users of mobile device firmware and software—constitutes a noninfringing use of the work, and but for the exemption that noninfringing use would be actionable under the anticircumvention provision, it seems safe to conclude that “users . . . are likely to be . . . adversely affected by \cite[section 1201]{17 USC § 1201} . . . in their ability to make noninfringing uses,”\textsuperscript{38} because 1201(a)(1) would obviously burden that noninfringing use.

\begin{footnotesize}
\begin{enumerate}
\item \textsuperscript{36} CTIA Comments at 60.
\item \textsuperscript{37} CTIA Comments at 23.
\item \textsuperscript{38} 17 U.S.C. § 1201
\end{enumerate}
\end{footnotesize}
CTIA implies that substantially chilling consumers’ ability to make this noninfringing use on their own by rendering it illegal under federal law would not by itself establish adverse impact, because wireless carriers will sometimes perform the unlocking operation at customers’ request. But carriers are often unwilling to unlock consumers’ devices; thus, disallowing individual consumers to unlock their own devices would have clear adverse effects that would extend beyond the mere hassle to consumers of having to ask their carriers to help them do something they could oftentimes accomplish on their own. These adverse effects would apply to consumers’ noninfringing use of a category of devices best described as “mobile devices.”

A. Wireless Carriers Are Often Unwilling to Unlock Consumers’ Devices

CTIA argues that “[a]n unlocking exemption is not necessary to promote competition and foster consumer choice,” noting that “carriers are willing to unlock handsets in a wide variety of circumstances” and citing to what it calls “liberal, publicly available unlocking policies.” However, an inspection of three carriers’ publicly available unlocking policies reveals a number of limitations:

- **AT&T** will not provide an unlock code to postpaid service customers who have not completed 90 days or more of active service with AT&T. It will not provide an unlock code during an unexpired “period of exclusivity associated with AT&T’s sale of the handset.”

- **T-Mobile** will not provide an unlock code to customers who have less than 40 days of active service with T-Mobile or

---

39 See CTIA Comments at 27.
40 CTIA Comments at 8.
41 Sprint does not appear to have a publicly available policy.
who have requested another unlock code in the past 90 days.\textsuperscript{43}

- **Verizon Wireless** makes no mention in its Customer Agreement of whether or not unlock codes will be provided for devices that use SIM cards.\textsuperscript{44} According to a February 26 article in *USA Today*, Verizon also requires that customers who wish to unlock their phones complete an extra online-activation step “in which the phone essentially gets permission from Verizon to use that card.”\textsuperscript{45}

It is particularly difficult to get a carrier to unlock certain kinds of devices, including iPhones:

- **AT&T** considers iPhones “and certain other devices”—an undefined category—“not eligible to be unlocked.”\textsuperscript{46}

- **Sprint** will unlock the micro-SIM slot on its iPhone 4S for subscribers who have been in good standing for 90 days or more. The unlock is incomplete, however—the “unlocked” device will only accept an international SIM, not one from a non-Sprint U.S. carrier such as AT&T.\textsuperscript{47}


\textsuperscript{45} The author explains that “[t]his added requirement compounds the difficulty of using a Verizon iPhone overseas—you can’t pick up any pre-paid SIM once you get there and have it work right away.” Rob Pegoraro, *How to Unlock Your iPhone 4S for World Travel*, USA Today (Feb. 24, 2012), http://www.usatoday.com/tech/products/story/2012-02-26/pegoraro-iphone-world-travel/53234322/1.

\textsuperscript{46} AT&T Policy.

\textsuperscript{47} Pegoraro, *supra* note 45.
• **Verizon Wireless** states that the iPhone 4 “is configured to work only with the wireless services of Verizon Wireless and may not work on another carrier’s network, even after completion of your contract term.”

Marc Weber Tobias, an investigative attorney and physical security specialist, explored the iPhone’s apparent lack of interoperability last year and wrote about his findings in a December blog post for *Forbes* called *How U.S. Carriers Fool You Into Thinking Your iPhone 4S Is Unlocked*. Tobias began by purchasing a new iPhone 4S from Best Buy for $800, “full retail so there would be no restrictions from Verizon with regard to unlocking the handset,” with plans to use it on networks operated by Verizon Wireless and other carriers. Tobias asked Verizon to unlock the device, was told it had been unlocked, and successfully used it on other carriers internationally. After that, however, he was astonished to discover that the device would not accept a SIM card from a regional domestic carrier in the Midwest United States. He concluded:

> What consumers need to understand is that there are actually four different versions of the iPhone 4S: Verizon, Sprint, AT&T, and Apple. Only the Apple phone, available from their stores or on-line, is fully unlocked and can be used on any carrier outside the United States. The other phones are permanently locked and cannot ever be used on another carrier in the U.S.

Moreover, despite having the hardware capacity to function on any GSM or CDMA network, even an “unlocked” iPhone 4S purchased directly from Apple ships with the ability to connect to GSM networks only.

---

48 Verizon Policy.
50 See Apple, iPhone 4S in Online Store, http://store.apple.com/us/browse/home/shop_iphone/family/iphone/iphone4s.
Some carriers even tell their customers that unlocking is impossible. For example, in a February 7, 2012 post in a forum on the Sprint website, a user asked, “I know that Sprint will unlock the SIM slot in the 4S for international use as long as you’re a customer in good standing. But any idea if they will unlock your phone completely once the contract is fulfilled so that you can use it with AT&T or T-mobile?” A Sprint representative posted in response, “The Sprint iPhone is made to work only on the Sprint Network and will not work on any other network. So it is not possible for it to be unlocked to work on another network.”

B. The Adverse Effects of Applying the Anti-Circumvention Provision Would Extend to Consumers’ Ability to Engage in Noninfringing Unlocking of “Mobile Devices”

CTIA argues that there is insufficient evidence in support of an unlocking exemption that would cover “mobile devices” rather than “telephone handsets.” But an exemption limited to “telephone handsets” would be underinclusive and cause unnecessary consumer confusion. As CU explained in its proposal, “the relatively basic telephone handsets of several years ago have evolved into a variety of dynamic multipurpose devices.” The phrase “telephone handset” no longer refers to a distinct and meaningful category of devices. It is more in line with current technology and consumer expectations to define the exemption in terms of “mobile devices.”

Indeed, it is likely already unclear to consumers whether some popular mobile devices sold locked to a particular carrier constitute “telephone handsets.” For example, a 3G-capable iPad is a handheld device that uses a cellular service network. It has a phone number assigned to it. And it is sold locked—a consumer ordering one from

---

52 CTIA Comments at 53–55.
53 CU Proposal at 2.
54 See Dan Moren, First Look: iPad Wi-Fi + 3G, MacWorld (Apr. 30, 2010), http://www.macworld.com/article/150966/2010/04/firstlook_ipad_3g.html (“Every iPad data plan does have a phone number associated with it, but if you try to call that
the Apple store online must select a network carrier before checking out and is
informed, “Your iPad will work only with the carrier you choose.”\textsuperscript{55}

Removing from such a device an artificial restriction that limits its operability to
a limited number of networks is a noninfringing use. This noninfringing use would be
adversely affected by a limitation on the unlocking exemption that makes it difficult for
consumers to discern whether or not they can unlock their devices. To avoid confusion
in this and similar situations, the language of the exemption should be crafted to clarify
that unlocking any “mobile device” is permissible.

III. CONCLUSION

For the foregoing reasons, Consumers Union asks the Librarian of Congress to
adopt its proposed exemption for mobile device unlocking.

Respectfully submitted,

/s/ ____________________________
Laura M. Moy*  
Angela J. Campbell  
Institute for Public Representation  
Georgetown Law  
600 New Jersey Avenue, NW  
Suite 312  
Washington, DC 20001  
(202) 662-9535  

Of counsel:  
Parul P. Desai, Esq.  
Communications Policy Counsel  
Consumers Union  
Dated: March 2, 2012  

Counsel for Consumers Union

\textsuperscript{55} See Apple, iPad in Online Store,  
* Admitted to the Maryland bar only; DC bar membership pending. Practice supervised
by members of the DC bar.