



GEORGETOWN LAW
INSTITUTE FOR PUBLIC REPRESENTATION

Hope M. Babcock
Angela J. Campbell
Brian Wolfman
Directors
Leah M. Nicholls
Senior Staff Attorney
Kelly D. Davis
Laura M. Moy*
Margot J. Pollans
Blake E. Reid
Staff Attorneys

600 New Jersey Avenue, NW, Suite 312
Washington, DC 20001-2075
Telephone: 202-662-9535
TDD: 202-662-9538
Fax: 202-662-9634

July 2, 2012

David O. Carson
General Counsel
U.S. Copyright Office
P.O. Box 70400
Washington, DC 20024

Via email: 1201@loc.gov

Re: Docket No. RM 2011-7
Exemptions to Prohibition on
Circumvention of Technological
Measures that Control Access to
Copyrighted Works

Dear Mr. Carson:

Consumers Union ("CU") respectfully submits this letter in response to the supplemental post-hearing questions you posed on June 21, 2012 to panelists who testified at the May 31 hearing on proposed exemption classes 6A, 6B, and 6C.

1. In its request for an exemption, Consumers Union argued that connecting a mobile device to a communications network is a "procedure, process, system, [or] method of operation" within the meaning of Section 102(b) of the Copyright

Act. It then stated that the feature of mobile device firmware or software that facilitates connectivity of a device to a communications network may be unprotectable under U.S. copyright law. If this is in fact the case, please explain why an exemption is necessary in order to use a mobile phone on a competing wireless carrier.

Even if, as argued by CU, connecting a mobile device to a communications network is a “procedure, process, system, [or] method of operation” within the meaning of Section 102(b) of the Copyright Act and the feature of mobile device firmware or software that facilitates connectivity of a device to a communications network is unprotectable under U.S. copyright law, an exemption is nevertheless necessary to ensure that consumers are able to unlock their own devices for use on the service network of their choice. This is because the technological protection measures that control access to the connectivity aspect of the firmware or software may in some cases control access to the entire mobile device operating system and/or other features, software, or firmware that are protectable.¹

Thus although the use an unlocking consumer makes of the firmware does not rise to the level of generating a derivative work, because any alterations to the firmware or software are made only to unprotectable functional aspects of that firmware, the circumventing action necessary to facilitate unlocking may in fact involve a technological protection measure that controls access to other, protectable, features.

2. Please comment on the proposed language of the alternative class set forth at p. 64 of CTIA’s comment:

Computer programs, in the form of firmware or software, that enable used wireless telephone handsets to connect to a wireless telecommunications network, when circumvention is undertaken by an

¹ See Proposal of Consumers Union, RM 2011-7, at 10 (Dec. 11, 2011) (explaining that “to unlock a mobile device, a consumer must often circumvent a protection measure that controls access to the entire mobile device operating system and/or other protectable content, such as wallpapers and ringtones.”).

individual customer of a wireless service provider who owns the copy of the computer program solely for noncommercial purposes in order to remove a restriction that limits the device's operability to a limited number of networks, or to connect to a wireless telecommunications network other than that of the service provider and access to the network is authorized by the operator of the network.

Computer programs, in the form of firmware or software, that enable ~~used~~ wireless telephone handsets to connect to a wireless ~~telecommunications~~ network, when circumvention is undertaken by an individual customer of a wireless service provider ~~who owns the copy of the computer program solely for noncommercial purposes in order to remove a restriction that limits the device's operability to a limited number of networks, or to connect to a wireless telecommunications network other than that of the service provider and access to the network is authorized by the operator of the network.~~

CU objects to the following features of the language of the alternative class set forth in CTIA's comment:

- **Inclusion of the word "used."** This is a restriction that unnecessarily limits consumers' ability to unlock their own devices. This restriction has no relation to device manufacturers' or service providers' rights under the Copyright Act.
- **"Telecommunications" rather than "communications" network.** What were historically "telecommunications" providers today commonly also provide information

services.² CU believes that this shift should be reflected in the language of the exemption so that consumers understand that both telecommunications and information services fall under the umbrella of “communications network.”

- **Restriction of the exemption to situations in which the individual undertaking circumvention “owns the copy of the computer program.”** As explained in previous submissions, CU believes this is a restriction that unnecessarily limits consumers’ ability to unlock their own devices in situations when they are unable to determine whether or not they “own” the copy of the computer program, or whether license terms that prevent them from owning the computer program are invalid on the basis of copyright misuse.
- **Inclusion of “solely for noncommercial purposes.”** As explained in testimony, the word “noncommercial” is confusing to consumers, many—if not most—of whom unlock their mobile devices for financial reasons.
- **Inclusion of ‘access to the network is authorized.’** This is a restriction that has no relation to device manufacturers’ or service providers’ rights under the Copyright Act. As discussed in CU’s reply comments, if carriers are concerned that approval of an anti-circumvention exemption for mobile device unlocking

² See 47 U.S.C. § 153(24) (“The term ‘information service’ means the offering of a capability for generating, acquiring, storing, transforming, processing, retrieving, utilizing, or making available information via telecommunications, and includes electronic publishing, but does not include any use of any such capability for the management, control, or operation of a telecommunications system or the management of a telecommunications service.”); see also 47 U.S.C. § 153(50) (“The term ‘telecommunications’ means the transmission, between or among points specified by the user, of information of the user’s choosing, without change in the form or content of the information as sent and received.”).

will encourage illegal access to wireless networks, they should be comforted by the fact that illegal access to wireless networks is already illegal. However, 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.

CU does not object to the following:

- **Restriction of the class to “wireless telephone handsets” rather than to “wireless devices” or “mobile devices.”** As explained in prior submissions, CU believes that “wireless telephone handsets” is a broad category that applies to any handheld mobile device using a wireless communications network. We merely requested that the language of the class be altered slightly to refer to “mobile devices” instead so as to minimize consumer confusion and bring the exemption language in line with modern terminology. However, we would not object to the retention of the current language if it were made clear that any handheld mobile device connecting to a wireless network is a “wireless telephone handset.”

CU thus offers the following proposal:

Computer programs, in the form of firmware or software, that enable ~~used~~ wireless telephone handsets to connect to a wireless ~~telecommunications~~ network, when circumvention is undertaken by an individual customer of a wireless service provider ~~who owns the copy of the computer program solely for noncommercial purposes~~ in order **to remove a restriction that limits the device’s operability to a limited number of networks,** or to connect to a wireless ~~telecommunications~~ network other than that of the service provider ~~and access to the network is~~

~~authorized by the operator of the network; and when circumvention is not initiated for the purpose of engaging in independently illegal activity.~~

CU believes that this proposed class strikes the right balance between copyright holders' interest in protecting mobile device firmware and software, and consumers' interest in making a noninfringing use of that firmware or software that enables them to bring their mobile devices with them from one service carrier to another. The alternative class proposed by CTIA leaves many confusing gaps and adds unnecessary language that could have a chilling effect on noninfringing uses.

4. It was recently reported in the press that both Sprint and Leap Wireless will be offering iPhones on a pre-paid plan basis. Please state whether these devices will be locked to their respective wireless networks.

The pre-paid iPhones offered by Sprint and Leap Wireless through their affiliated subsidiaries Virgin and Cricket are locked to these respective networks for domestic use. Virgin's iPhone is also locked for international use, but Cricket's prepaid iPhone is only SIM-locked to prevent use on other domestic wireless carriers; it is not similarly locked for international SIM-card use.³

5. Please indicate, in percentage terms or, if percentages are unavailable, in as accurate a fashion as possible, how many mobile wireless providers other than AT&T, Verizon, Sprint, and T-Mobile now use mobile phone locks to keep customers on their respective wireless networks.

CU believes that almost every wireless service provider uses mobile device locks to keep consumers on their respective networks. While statistics regarding the

³ Rob Pegoraro, *Cricket or Virgin: What's Best iPhone Deal?*, USA Today, June 16, 2012, available at <http://www.usatoday.com/tech/news/story/2012-06-17/pegoraro-iphone-cricket-virgin/55619450/1> ("Cricket says it will keep the SIM (Subscriber Identity Module) card slot on its iPhone 4S unlocked for international use. Virgin, by contrast, will keep its iPhone locked, spokeswoman Jayne Wallace said...But with Cricket, publicist Greg Lund confirmed, you could buy an iPhone, pay for a month of service to activate it on Cricket's network, then take the device on the plane and pop in a prepaid SIM when you arrive overseas. The carrier will, however, keep its iPhone locked against use with other carriers in the U.S.").

amount of wireless service providers that lock devices to their respective networks are unavailable, a survey of the purchase and use Terms and Conditions of six providers⁴—Metro PCS, Boost Mobile, Cricket, Net10, Tracfone, and Credo Mobile⁵—all make references to the fact that their devices are locked or designed for exclusive use on their respective networks.⁶

Even companies offering pre-paid and “contract-free” wireless services lock their devices to keep customers from using their devices on other networks. These companies often promote the fact that they do not require consumers to contract with the provider to purchase a mobile device, connoting that consumers will be free to easily switch providers. However, the locks on the mobile devices offered by the companies keep many consumers tied to a single provider. For example, Metro PCS, which offers “contract-free” pre-paid wireless service and explicitly accepts unlocked phones for use on its network, locks the mobile devices it sells for exclusive use on its network.⁷

⁴ In accordance with the scope of the question presented, the big-four providers, AT&T, T-Mobile, Verizon, and Sprint (along with its Virgin Mobile affiliated provider), were excluded from the survey.

⁵ Metro PCS Terms and Conditions, available at <http://www.metropcs.com/metro/tac/termsAndConditions.jsp?terms=Terms%20and%20Conditions%20of%20Service>; Boost Mobile Terms and Conditions, available at <http://www.boostmobile.com/support/services-policies/terms-conditions/>; Cricket Terms and Conditions, available at <http://www.mycricket.com/support/terms-and-conditions>; Net 10 Terms and Conditions, available at http://www.net10.com/content/terms_conditions.jsp; Tracfone Terms and Conditions, available at http://www.tracfone.com/e_store.jsp?task=buyphone; CREDO Mobile Customer Agreement, available at <http://www.credomobile.com/misc/Customeragreement.aspx>.

⁶ For example, CREDO Mobile’s Customer Agreement says, “[w]ithout alteration, your phone will not accept the services of any mobile provider other than CREDO.” <http://www.credomobile.com/misc/Customeragreement.aspx>. Boost Mobile’s Terms and Conditions of purchase state, “[t]his Device is sold exclusively for use with our Service and in other coverage areas that we may make available to you. As programmed, it will not accept wireless service from another carrier,” <http://www.boostmobile.com/support/services-policies/terms-conditions/>.

⁷ Metro PCS Terms and Conditions, available at <http://www.metropcs.com/metro/tac/termsAndConditions.jsp?terms=Terms%20and%20Conditions%20of%20Service> (“If your wireless device was purchased from MetroPCS or an authorized MetroPCS dealer, the wireless device has a software programming lock that will prevent the wireless device from operating with other compatible wireless telephone carriers' services”).

Of counsel:

Parul P. Desai, Esq.
Communications Policy Counsel
Consumers Union
1101 17th Street, NW
Suite 500
Washington, DC 20036
(202) 462-6262
PDesai@consumer.org

Margo Varona
Georgetown Law Student

Dated: July 2, 2012

CC:

Bruce Joseph, Esq.
Steven Berry, Esq.

Respectfully submitted,

/s/

Laura M. Moy*
Institute for Public Representation
Georgetown Law
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9535
lmm258@law.georgetown.edu

Counsel for Consumers Union

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