Thursday, 1 December 2011

Office of the General Counsel
U.S. Copyright Office
James Madison Memorial Building
Room LM-401
101 Independence Ave., SE
Washington, DC 20559-6000

BY ELECTRONIC SUBMISSION
http://www.copyright.gov/1201/comment-forms/comment-submission.html

Re: Notice of Inquiry, 76 Federal Register 60398, 29 September 2011
Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies
Docket Number RM 2011-7

Dear Sirs:

I. Proposed Class of Copyrighted Works for which Exemption is Requested

Exemption from Section 1201(a)(1)(A) (the "Anticircumvention Provision") of the Digital Millennium Copyright Act (DMCA) is requested for the following class of works within the statutory class of literary works:

> "Wireless Network Interoperability Programs." Computer programs, in the form of firmware or software, including data used by those programs, that enable wireless devices to connect to a wireless communications network, when circumvention is initiated by the owner of the copy of the computer program principally in order to connect to a wireless communications network and access to such communications network is authorized by the operator of such communications network.

I refer to this proposed exemption category as "Wireless Network Interoperability Programs" because the principal purpose for the exemption is to legitimately enable a particular wireless device to be interoperable with a new wireless communications network and the software and other systems associated with that network. This proposed exemption is worded substantially the same as the third class of works that was exempted by the Librarian of Congress in 2010, with a few exceptions as revealed in the following redline version that compares to the 2010 exemption language. Three conceptual

changes represented by the newly proposed wording are then described in more detail further below.

> "Computer programs, in the form of firmware or software, including data used by those programs, that enable ~~used~~ wireless ~~telephone handsets~~ devices to connect to a wireless communications network, when circumvention is initiated by the owner of the copy of the computer program ~~solely~~ in order to connect to a wireless ~~tele~~communications network~~s~~ and access to ~~the~~ such communications network is authorized by the operator of ~~the~~ such communications network."

The first notable change is for purposes of clarity – addition of the phrase "*including data used by those programs*" – which has the same intent but is more accurate. While most of the strategies used to control wireless network interoperability involve accessing firmware or software on the device, the required adjustments for interoperability often do not require changing large sections of code but, rather, accessing and changing the data that is used by such code. Granted, accessing software assumes access to the data used by such software, but clarity is needed, particularly while there are copyright theories that reach to the level of protecting compilations of data almost at the same level as code.

Likewise, recognizing technological evolution of wireless communication, we also propose an exemption that is broader than programs for just "*used*" "*telephone handsets*." Instead, we propose phraseology of "*wireless devices*" or "*wireless communication devices*," or the equivalent. Perhaps most wireless devices might still be considered telephone handsets, but this is rapidly becoming an outdated perspective. A tremendous number of products that represent substantial commerce in the marketplace utilize wireless communication without being considered either "*telephone*" or "*handsets*" in what might be the ordinary sense of those words. Tablets and notebook computers, for example, might be viewed as significant exceptions to the "*handset*" characterization, and a vast number of personal digital devices are also using wireless communication networks to convey data in various industries without technically being characterized as a phone or telephone. The definitions need to be adjusted to remain in line with current commerce now, as well as over the next three year period.

Finally, elimination of the "solely" restriction is needed to provide clarity, particularly given the inherent uncertainties presented to the average consumer. Granted, the purpose of connecting to a particular wireless network is indeed the principal purpose for which such access is required, but "solely" creates confusion for judges and consumers alike whenever someone acknowledges that the desire to switch networks also has another purpose, regardless of how trivial. The word "solely" might often be understood as an absolute, which would rule out cases where the principal purpose of switching networks is secondary to a purpose of serving others, or facilitating a business relationship, or making money, or whatever. While many carriers and technicians will help an owner of a wireless device to perform a network switch if the owner so desires, such secondary purposes are commonly assumed to still not depart from the "solely" intent, but clarity is needed. Therefore, we request that the "solely" language of the current exemption be deleted or, in the alternative, changed to a more accurate word such as "principally," to ensure clarity that the purpose language is not so restrictive as to not

cover them or their helpers even if other purposes are being served secondarily in the process.

II. COMMENTING PARTY -- YOUGHIOGHENY COMMUNICATIONS, LLC

Youghiogheny Communications, LLC ("Youghiogheny") is a Delaware limited liability company that has been parent to regional wireless carriers and continues to own significant interests in wireless carrier operations. While Youghiogheny's operating companies have provided new wireless devices for many of their customers, they have also been willing, on request, to let customers continue to use devices that the customers already own.

III. ARGUMENT SUMMARY

Continued exemption is needed for Wireless Network Interoperability Programs because carrier locks that are commonly associated with such programs prevent them from being modified so the devices can be used on other networks, thereby dramatically reducing competition and hurting American consumers as well as our landfills. Redirecting Wireless Network Interoperability Programs does not infringe the associated copyrights, and yet it typically cannot be accomplished without unlocking the carrier locks. Meanwhile, the exemption language is out of date and presents dramatic uncertainty to consumers and those that are willing to help them. The exemption therefore remains imperative, and clarity is needed.

IV. FACTUAL SUPPORT / DETAILED ARGUMENT

A. The Prevented Activities & The Good They Represent

Many customers come to wireless carriers after having their service discontinued with a larger carrier. If such a customer chooses to continue using a device bought from their prior carrier, at some point before wireless service can be provided through the new carrier, the programming that controls the device must be accessed and adjusted to connect to the new carrier's network. A problem is raised if the device has a carrier lock[1] to tie the device to the customer's prior carrier. Mega-carriers typically include some form of carrier lock embedded in the programming for the devices that they sell to their customers – with or without the customer's knowledge or consent. So long as a carrier lock is not circumvented, it prevents the new carrier from accessing programs that control what carriers and/or networks the device can connect to. As a result, even though device

[1] Popular carrier locking strategies include: (i) SPC (service provider code) locking, which has been used by Verizon Wireless and Sprint-Nextel, employs codes derived from an algorithm that uses the device's electronic serial number (ESN) and prevents reprogramming of a device unless the programmer first inputs the correct SPC code; (ii) SOC (system operator code) locking, which has been used by AT&T Wireless (formerly Cingular), requires the matching SOC code to be entered into the device before it can be changed to another carrier's SOC code; (iii) Band Order Locking, which restricts the frequencies on which devices will operate to those licensed for the carrier that implements the lock; and (iv) SIM (subscriber information module) card locking, which is used by T-Mobile to prevent use of other carriers SIM cards on mobile phones that it sells, and which can be unlocked by entering an eight-digit code number so that the device will then operate with a SIM card for any network.

owners have the right to use their old devices after legitimately switching from one carrier to another, they are not able to do so without circumventing the carrier locks.

While Youghiogheny has been involved in the carrier marketplace for a number of years, we reject the notion that carrier locks are needed to help protect margins in the wireless communication services market. Just the opposite, by allowing customers to find ways of properly unlocking their devices (as permitted with the 2006 and 2010 exemptions and the clarified exemption proposed here), barriers to competition come down, innovative start-up carriers are able to enter the market, and free market factors start allowing customers cost savings as well as choice. Now, with the ability to unlock their own devices, consumers are able to choose amongst numerous competing carriers whether to go for more features and service or whether to go for a discount option in order to save money and minimize waste. The result democratizes the wireless landscape and allows expansion of service to consumers at all income levels. The removal of barriers to competition, in turn, allows device subsidization to become a choice rather than the *de facto* standard that has favored mega-carriers. Plus, consumers are able to choose amongst all competitors rather than being forced to only buy equipment from the network that they are tied to, again increasing competition and ultimately allowing customers to save on costs. Without unjust restraints in wireless markets, the overall cost of obtaining service is reduced, service becomes more and more available for low income consumers, and consumer choice increases both for devices and for carrier services.

Fortunately, as a result of the 2006 and 2010 DMCA exemptions and litigation settlement agreements pressured by application of those exemptions, several of the mega-carriers have reportedly started allowing customers to obtain access to their device operating programs in order to switch a device from one network to another. Nonetheless, this process is needlessly tedious, and most consumers still cannot use their device on another carrier network without circumventing a carrier lock, even after fulfilling his or her contractual obligations with the carrier that sold them the device.

The 2006 and 2010 exemptions that allowed consumers to unlock their devices are good for both the market and the consumers. Irrespective of whether there was improper intent in establishing a marketplace of customers tied to individual mega-carriers, carrier locks dramatically reduce the benefits of free market forces within each silo of customers that are captive to a particular carrier. Without realistic options for switching carriers, carrier locks leave captive customers with fewer options and ultimately having to pay higher prices from the sole source of supply that they are tied to.

B. Prevented Activities Have No Connection to Potential Infringements

But for the prohibition of the Anticircumvention Provision, device owners who wish to switch service providers would not infringe the copyright rights in the device programming. Directing the Wireless Network Interoperability Programs to use a different network or carrier typically does not require duplicating the device programming or exercising any of the other basic rights afforded by copyright. Rather, in the classic idea/expression context of copyright law, changing the network or carrier is more like changing the factual information included in a copyrighted work rather than changing the protectable expression of that work.

Moreover, even if any necessary reprogramming rises to the level of creating an adaptation of copyrighted device programming, Section 117 of the Copyright Act provides that such adaptation does not infringe the associated copyrights. Particularly, Section 117(a)(1) expressly provides that "it is not an infringement for the owner of a copy of a computer program" to adapt it so long as the adaptation is created "as an essential step in the utilization of the computer program in conjunction with a machine."[2] The owner of equipment that contains a copy of a program, hence, has what has been called the "right of adaptation," which includes the right to add features to the program that were not present at the time of acquisition, to suit the owner's needs. For Wireless Network Interoperability Programs, this means that the device owner clearly has the non-infringing right to reprogram their device in order to switch carriers.

C. Bulk Unlocking Schemes Are Different

Notwithstanding the above, it is important to distinguish legitimate network switches from bulk unlocking schemes, such as those that have been addressed in various court proceedings initiated by prepaid service providers over the last several years. Stereotypically, bulk unlocking schemes are questionably-legal, coordinated efforts to buy up hundreds or thousands of subsidized devices for the purpose of unlocking them *en masse,* without any intent to ever use the devices on the network that subsidized their purchase. Such unlocked devices can then be resold in bulk quantities through wholesale distribution channels both domestically and overseas. Unlike the case of redirecting a device's individual network connection, we respectfully submit that bulk unlocking schemes should not fall within the scope of the proposed exemption because such access is not thought to be "principally in order to connect to a wireless communications network and access to such communications network is authorized by the operator of such communications network."

D. Substantial Adverse Effects on Non-Infringing Uses

Without continuation and clarification of the requested exemption, a device owner who stops using a mega-carrier's service would typically only have two realistic options when that mega-carrier has embedded carrier locks in the device programming – either (1) abandon the non-infringing rights and reinstate service with the former carrier, or (2) abandon the non-infringing rights and throw the device into a local landfill. Either way, the impact to the non-infringing rights is terminal.

The resulting harm is substantial, not only through forced termination of the non-infringing activity, but also in presenting substantial risks and uncertainties for smaller carriers like Youghiogheny that let customers who want to save money continue use of their prior devices rather than force them to buy new ones. Carrier locks allow mega-carriers to minimize competition and discourage innovation in the mobile communication market. As a result, customers get poorer service, higher prices and fewer solutions. Without the proposed exemption, the Anticircumvention Provision would have a critical adverse impact on the wireless communication network market, our environment, and our

[2] 17 U.S.C. §117(a)(1)(2007).

consumers, particularly on those who cannot continue paying for service with a mega-carrier during difficult financial times.

V. Concluding Remarks

The benefits of the 2006 and 2010 exemptions in overcoming the problems outlined here and elsewhere more than demand a continuation of that exemption. Irrespective of whether mega-carriers appreciate the good in competition, the exemption has allowed non-infringing access to work for good all around – good for both consumers and carriers. Because device unlocking is a non-infringing activity that serves such substantial needs in the marketplace, and because section 1201(a)(1)(A) would otherwise prohibit classic device unlocking, we respectfully request grant of the proposed exemption.

We trust it will be remembered that the Anticircumvention Provision was promulgated for the purpose of creating a practical limit on activities that were precursors to copyright infringement. That, however, is not the case with the carefully tailored exemption presently proposed. Congress recognized the potential for adverse effects and chose to create the exemption rulemaking process as a "fail-safe mechanism," to not just monitor the effect of the Anticircumvention Provision, but to remedy situations where a substantial adverse effect on non-infringing uses is demonstrated. In the present case, the prohibited switching of network carriers does not itself involve impermissible copyright infringement. To the contrary, reprogramming your device's copy of a Wireless Network Interoperability Program, or the data that is used by that program, is a permissible non-infringing activity that indeed should be encouraged because of its benefits for the market, the consumers and the environment.

We respectfully request that the Librarian of Congress establish the proposed exemption for the next triennium under the DMCA provisions.

Youghiogheny Communications, LLC

By: 

Paul Posner, President