Cowan, Liebowitz & Latman, P.C.

Law Offices

1133 Avenue of the Americas • New York, NY 10036-6799

(212) 790-9200 • www.cll.com • Fax (212) 575-0671

Morton David Goldberg
Direct (212) 790-9253
mdg@cll.com

September 11, 2006

David O. Carson, Esq.
General Counsel
United States Copyright Office
James Madison Memorial Building
101 Independence Avenue, SE
Washington, D.C. 20559-6000
daca@loc.gov

Re: Copyright Office Docket No. RM 2005-11:
Exemption to Prohibition on Circumvention of Copyright
Protection Systems for Access Control Technologies

Dear Mr. Carson:

Mr. Steven J. Metalitz has informed our client CTIA – The Wireless Association® ("CTIA") of your letter of August 14, 2006 to him and Ms. Granick, seeking "additional and more detailed information" in the Office's DMCA Section 1201 Rulemaking relating to a proposed exemption for "computer programs that operate wireless communications handsets." And CTIA understands from Mr. Metalitz that he is responding to your letter as requested.

As your letter acknowledges, his clients in this proceeding do not include "handset manufacturers, telecommunications service providers or others directly involved [in] the activity that is the subject of the proposed exemption." Because CTIA does represent companies directly involved, CTIA wishes to take this opportunity to complement Mr. Metalitz's response by supplying the additional information necessary for you to receive full answers to your questions.

CTIA acknowledges, as your letter states, that "these questions have arisen at a fairly late date in this rulemaking proceeding ...." However, in light of the Office's recent request for further information and two developments that have only recently come to CTIA's attention, CTIA respectfully submits the attached information for consideration by the Office at this time in the belief that the information may significantly affect the Register's recommendation.

CTIA has learned of a criminal complaint filed by the government on August 16, 2006 that highlights the importance of access control measures on wireless devices in the context of the proposed exemption. The complaint was filed in the United States District Court for the Eastern District of Michigan in United States v. Othman, No. 06-MI-30401. In the complaint, the government alleges that several persons had participated in an organized scheme to defraud wireless companies by circumventing access control measures on pre-paid phones in violation of 17 U.S.C. Secs. 1201(a)(1)(A) and 1204(a), in order to sell them at market (non-subsidized) prices outside of the United States.

In the second development, an unrelated matter, but also relating to the exemption proposal, CTIA has recently learned that the proposer, The Wireless Alliance, is now listing CTIA as its "partner" in the proposer's business of recycling used wireless devices, although there is no such relationship whatsoever; and by separate letter to the proposer, CTIA is now demanding that the proposer immediately cease and desist its misrepresentation and its infringement of CTIA's service marks.

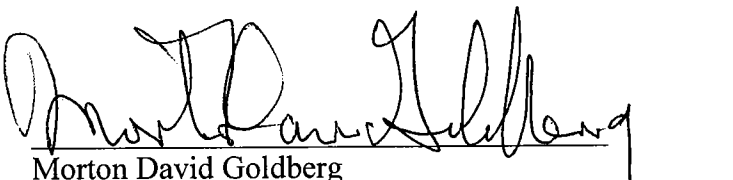
In light of these recent developments, CTIA believes it all the more necessary that the Office record on the issue of the exemption proposal now be made complete and accurate.

In submitting this information, CTIA of course speaks only for its members, not for Mr. Metalitz's clients.

We believe that the information demonstrates why the proposed exemption should not be granted, and why the Office is not the appropriate forum for proposals to restructure the wireless industry.

Respectfully submitted,

COWAN, LIEBOWITZ & LATMAN, P.C.,



Morton David Goldberg

Jason D. Sanders

Enclosure

cc: Jennifer S. Granick, Esq.
Stanford Law School Center for Internet & Society
Cyberlaw Clinic
559 Nathan Abbott Way
Stanford, CA 94305
jennifer@law.stanford.edu

Steven J. Metaliz, Esq.
Mitchell Silberberg & Knupp LLP
2300 M Street, N.W., Suite 800
Washington, D.C. 20037
met@msk.com

UNITED STATES COPYRIGHT OFFICE
Copyright Office Docket No. RM 2005-11

Regarding Proposal for Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies

Information Submitted
on Behalf of

CTIA – THE WIRELESS ASSOCIATION®

Complementing Response to Copyright Office Request of August 14, 2006 for Further Information

Submitted by:

Morton David Goldberg
mdg@cll.com
Jason D. Sanders
jds@cll.com
COWAN, LIEBOWITZ & LATMAN, P.C.
1133 Avenue of the Americas
New York, NY 10036-6799
(212) 790-9200

Attorneys for CTIA – The Wireless Association®

Of counsel:

Michael F. Altschul
Senior Vice President and General Counsel
CTIA-The Wireless Association®
1400 16th Street, NW Suite 600
Washington, DC 20036

QUESTIONS PROPOUNDED IN COPYRIGHT OFFICE LETTER OF AUGUST 14, 2006

(1) Explain how each of the types of software locks controls access to a copyrighted work.

(2) Identify and describe the copyrighted work (or works) with respect to which access is controlled by the software lock. (a) Who is the copyright owner of that copyrighted work? (b) If the software lock controls access to only a portion of the work(s), identify both the work(s) and the portion(s) of the work(s).

(3) What information, process or treatment must be applied in order to gain access to that copyrighted work(s) (or the identified portion(s) of the work(s)).

(4) In what respect is access to that copyrighted work controlled by the software lock, including (but not confined to): (a) what is the nature of the access to the copyrighted work that is controlled by the software lock?

(5) How does the software lock control such access to the copyrighted work?

(6) Describe whether and how the authority of the copyright owner of the copyrighted work is implicated in the operation of the software lock, including (but not confined to):

(a) who (e.g., the firmware manufacturer, the handset manufacturer, or the telecommunications service provider) installs and/or activates the software locks on the cellular phone handsets;

(b) whether the software locks are applied "with the authority of the copyright owner," and

(c) if the software locks are not installed by the copyright owner, (i) what is the relationship between the copyright owner and the person who installs the software locks; (ii) are (and if so, in

what respect are) the software locks applied with the permission of the copyright owner;

(d) In what respect has the copyright owner authorized the application of information, or a process or a treatment, to gain access to the work.

(7) In what circumstances, if any, is access to the copyrighted work authorized by the copyright owner

[(8)] Whether the software locks in question are technological measures that "effectively control access to a work" as defined in §1201(a)(3)(B)

CTIA – The Wireless Association® ("CTIA") submits these comments in connection with the Copyright Office's October 3, 2005 Notice of Inquiry[1], and more specifically in response to the letter dated August 14, 2006, from David O. Carson, General Counsel of the Copyright Office, to Jennifer Granick, Esq. and Steven Metalitz, Esq.

B. STATEMENT OF INTEREST

CTIA is a non-profit trade association that promotes the interests of the wireless industry, representing both wireless carriers and manufacturers. Membership in the organization covers all Commercial Mobile Radio Service (CMRS) providers and manufacturers, including carriers that are licensed by the Federal Communications Commission to provide cellular, broadband PCS, and ESMR services, as well as providers and manufacturers of wireless data services and products. CTIA's members serve over 95% of the more than 210 million wireless customers in the United States, In addition, CTIA's membership includes the major suppliers of the handsets used by wireless subscribers to access wireless networks and the broad variety of content and applications provided by wireless carriers and others in the wireless "ecosystem."[2]

CTIA opposes the exemption of "computer programs that operate wireless communications handsets" proposed by The Wireless Alliance. Neither the facts nor public policy support such an exemption for the software locks described in the comments and

---

[1] *See* Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 70 Fed. Reg. 57526 (2005).

[2] CTIA has recently learned of the unauthorized use of CTIA's U.S. Registered Service Marks by the proposer of the exemption, The Wireless Alliance. On proposer's website, http://www.thewirelessalliance.com/about_partners.html, the proposer lists CTIA as a "partner" in the proposer's recycling business, but there is no such relationship. By separate letter to the proposer, CTIA is now demanding that The Wireless Alliance immediately cease and desist its infringement of CTIA's service marks.

testimony of The Wireless Alliance. For the reasons set forth below, CTIA believes the proposed exemption should not be granted, and respectfully submits that the Office is not the appropriate forum for proposals to restructure the wireless industry.

C. COPYRIGHT OFFICE QUESTIONS

(1) Explain how each of the types of software locks controls access to a copyrighted work.

Various Access Control Measures Are Used

Wireless service providers use various technological measures to control access to the copyrighted works that they own or license from other copyright owners ("software access control" methods). Among these methods are software locks. For example, carriers whose network technology requires use of a "subscriber identity module" card (SIM card), may implement a "SIM subsidy lock," while others use a "service programming code" (SPC) and/or master subsidy lock (MSL) as their method of software access control.[3]

Whichever method is used to control access to the copyrighted works on the handset, failure to properly authenticate the user may deny the user virtually all access. Once there has been verification, however, the phone user is given access to the copyrighted applications and other software on the handset, as well as to the copyrighted works on the carrier's network,

[3] Wireless carriers in the United States have deployed a variety of digital technologies to provide wireless service. At present, the two most dominant technologies are GSM (Global System for Mobile Communications which is a time-division multiple access technology), and CDMA (Code Division Multiple Access). Among the national wireless carriers, Cingular and T-Mobile use GSM technology; while Verizon, Sprint, and Alltel Wireless use CDMA technology. SIM cards are used in wireless handsets that work on GSM networks; CDMA handsets use SPC and/or MSL as their method of software access control. Proposer also refers to system operator code (SOC) and band order locking. Similarly to other locks, SOC locks prevent third parties from reprogramming a handset. This type of locking is less frequently used today, though at least one carrier uses a similar system to prevent reprogramming of its pre-paid phones. Band order locking is not commonly used by major carriers in the current market in the United States.

including the network software for voice communication and non-voice data transmissions, and other copyrighted works such as music, video, games and other content.

In a SIM card system, the software access control requires that SIM software on the handset receive certain confirmatory information from data stored on the SIM card, in order to give the user access to copyrighted works on the handset or that are otherwise accessible over a carrier's network. The SIM card stores a variety of information specific to the handset's user, such as subscription information, personal preferences, phone book information, and text messages, in addition to information identifying the wireless telecommunication carrier (the "mobile network code" (MNC) that issued the SIM card to enable the handset to operate on its network). The card contains a copyrighted program and a repository for information necessary to answer queries from handset software or network software.

To prevent fraud and the theft of wireless service, wireless carriers must authenticate and authorize all wireless devices. SIM card verification controls access to the carrier's network software by requiring both that the proper phone is being used (*e.g.*, a phone with the proper MNC) and that the phone is authorized to access the carrier's network.

In order to effectively control access to the copyrighted works, the SIM card is engineered through encryption, password protection and other methods, to be very difficult to penetrate through hacking or other circumvention. In particular, the verification code and algorithm are known only to the SIM card and a suitably programmed phone that enables the SIM card and the handset to work together to authorize user access. That access is necessary if the user is to benefit from either the software on the handset or the network software (with further access to the content software linked through the network).

For carriers using SPC and MSL codes to control access to the handset's software, the handsets are similarly programmed to communicate information specific to the handset's user, including information relating to the customer's rights to access the network and other subscription information that affects the services the network provides to the customer.

The SPC and/or MSL locks effectively control access to certain critical computer programs (the "programming module") in a handset by using a unique, carrier-generated code. For at least some carriers that use SPC and/or MSL codes, the codes themselves are considered confidential and proprietary. The programming module also contains the handset's mobile identification number,[4] roaming lists,[5] and other technical information.

If an SPC or MSL lock is not activated (*i.e.,* is left at the 000000 default value), the programming module of the handset may be easily accessed. But if an SPC or MSL lock is activated with a unique code, the lock usually can be opened only by obtaining the code from the locking carrier.

Whether and to what extent SPC locks are used, if at all, varies among CDMA wireless carriers. For example, at least one carrier does not lock its handsets, and instead uses a default value that allows open access to the programming module of phones purchased by its "post-pay" customers, who are under term contracts and make up the vast majority of the carrier's customer

[4] The "mobile identification number" along with the "mobile directory number" is the customer's ten digit phone number.

[5] Roaming lists enable handsets to select the network(s) preferred by the serving carrier when the customer is "roaming" (*i.e.,* outside of the carrier's home service area).

base.[6] Other CDMA carriers utilize SPC locks to restrict access to the programming module, requiring input of the carrier-generated code.

For the vast majority of the phones that use a software access control method, access to the copyrighted works is controlled effectively in that the failure to satisfy the authentication measure generally bars access to the copyrighted works on the handset, the copyrighted network software that admits the device to the wireless carrier's network (with the exception of 911 emergency calling), and the copyrighted content thus made available to the consumer.

Access Control Measures Also Function As Anti-Theft Measures

Both the SIM and SPC/MSL verification processes also act as "anti-theft" measures. If the access control can be circumvented, the phone can then be reprogrammed so that it can be used on any compatible network (*e.g.,* GSM or CDMA) that uses at least one of the bands to which the transceiver tunes. Many of the current phones have the technology to work in more than 250 countries around the world, where they are easily marketable beyond the reach of U.S. authorities and never recovered.

In the United States, wireless carriers typically discount (or subsidize) the price of the handset as an inducement to attract new customers to their network. Since customers in other countries typically pay the full price of a handset, absent the SIM and SPC/MSL verification processes, there would be an arbitrage opportunity in exporting discounted handsets from the United States for sale in countries, such as Mexico, where discounting is not prevalent.

---

[6] However, this carrier locks the handsets it provides at a discounted price to its "pre-paid" customers.

These technological measures make it feasible for carriers to subsidize the cost of handsets and thus make the entry into the wireless services market for new customers "more palatable." *In re Wireless Tel. Servs. Antitrust Litig.*, 385 F. Supp. 2d 403, 410 (S.D.N.Y. 2005). Some carriers choose to invest in better quality handsets as a marketing differentiation, and the locking mechanism allows them to put high quality devices in customers' hands, while protecting the carrier's investment. Carriers recoup the subsidy during the lifetime of the user's activation on the network. While carriers typically require customers to enter into a fixed term contract, often with an early termination fee for customers who terminate their contract early, there are many customers from whom the carriers do not collect an early termination fee.[7] Removing the DMCA liability for defeating the lock would remove one of the few mechanisms the carriers have to reduce this sort of revenue loss and fraud.

Allowing circumvention of the verification process would make handsets (especially the more sophisticated and expensive ones) more vulnerable to theft and thereby significantly expand the market for stolen phones. Indeed, the theft of handsets has become a problem in the United States, and the circumvention of technological measures contrary to 17 U.S.C. §§1204(a) and 1201(a)(1)(A) may now be a key element of law enforcement's ability to prosecute these crimes. The government's recent filing of a criminal complaint in Michigan on August 16, 2006 has highlighted the importance of access control measures in this context. In United States v. Othman, No. 06-MI-30401 (E.D. Mich), a criminal complaint was filed against several persons

[7] Pre-paid customers typically do not have a contract with their carrier, and even post-paid customers have a choice of carriers and service plans that offer a discounted handset without an early termination fee. Moreover, even where the customer has entered into a contact that includes an early termination fee, carriers cannot collect the fee from customers who are insolvent, have relocated, or have fraudulently acquired service under a stolen identity (with the intent, having acquired the handset at a subsidized price, to evade the contractual term of service and resell the phone for a profit).

who are alleged to have participated in an organized scheme to defraud wireless companies by circumventing the access control measures of pre-paid phones in order to sell them at market (non-subsidized) prices. This recent event makes it all the more important and necessary for CTIA to present the information herein to the Copyright Office at this time.

Software access controls are essential to carriers and other companies that market "pre-paid" wireless service. These companies sell the wireless handsets for below their own cost with the expectation of recouping that investment over the lifetime of use of the device. Software locking helps to ensure that these heavily subsidized handsets are not fraudulently switched to another system or carrier -- or merely sold on the open market as "unlocked" -- depriving the original seller of its subsidy investment. Allowing circumventions would also greatly reduce the likelihood that people who do not wish to sign a contract for wireless service would be able to obtain a discounted handset along with their wireless service.

(2) Identify and describe the copyrighted work (or works) with respect to which access is controlled by the software lock. (a) Who is the copyright owner of that copyrighted work? (b) If the software lock controls access to only a portion of the work(s), identify both the work(s) and the portion(s) of the work(s).

<u>The Technological Measures Control Access to a Broad Spectrum of Copyrighted Works</u>

Software on the handset may consist of handset operating systems, applications and additional content. Increasingly, these types of software are becoming integrated.

Copyrighted works in the form of handset operating systems are typically preinstalled on the handset at time of purchase, while updates may be downloaded at a later time. Handset operating systems are typically owned by and proprietary to the handset manufacturer/vendor. Relying on the anti-circumvention protection of technological measures, however, wireless

carriers are increasingly focusing on developing handset systems that integrate operating software with other applications and services, as part of unique product and service offerings to consumers. These offerings include those associated with unique and proprietary handset user experiences and handset operation. Such carrier-owned systems will likely be highly confidential and proprietary to those carriers.

Application software on the handset typically consists of email and text messaging applications, phonebook/directory applications, and similar applications. They are usually preinstalled on the handset, but may also be downloaded to the handset at a later time. Application software is usually owned by and proprietary to handset manufacturers, but may also be developed and owned by third-party content and application developers, who then license their copyrighted material through handset manufacturers or directly to wireless telecommunications carriers.

Third-party application software includes a wide variety of applications, such as the copyrighted gaming software needed to play on-line videogames. Handset manufacturers/vendors may own and license such applications, but typically such applications are offered to a wireless telecommunications carrier's customers as part of specific offerings. These applications may be preinstalled, but are usually downloaded to a handset at a later time. Other files with copyrighted works that are accessed typically include content such as ringtones, photographs, wallpapers, music and videos. Some content files are preloaded and reside on the handset, while others are downloadable to the handset.

Much of the copyrighted content described above may reside on the device, but some will be on the carrier's network and some with a third party, to whom the carrier provides a

connection for the consumer. In general, a ringtone or a standalone game is downloaded from a third party, but then resides self-sufficiently on the handset. Other content may have the purpose of communication with a community of wireless on-line users (such as the copyrighted text and graphics dating and chat services). On the vast majority of handsets, access to this content requires prior identification of the wireless user by authentication through the process controlled by a SIM card or similar technological measure, and circumvention of the measure would facilitate infringing uses of these copyrighted works as well as the copyrighted works comprising the network software.

There is significant content not on the handset that is either part of or available through copyrighted network software. In addition to controlling access to handset software described above, software access controls protect against unauthorized access to network software, and network software is increasingly used to access content in and through the carrier's network. Thus, control of access to the network software also controls access to that content.

As stated above, access control measures protect against unauthorized access to handset software and network software, which may include operating systems, content and applications. Increasingly, these are becoming intertwined to enhance the consumer's ease of use, and thereby make more copyrighted works easily available to the consumer. The copyrighted works that comprise a carrier's handset software and network software are characterized by extremely complex and sophisticated programming far beyond the comparatively trivial computer programs that consumers may encounter in over-the-counter devices such as printers and garage-door openers.

Copyright Owners Increasingly License Rights Exclusively to a Given Carrier

Wireless carriers, more and more, are reaching exclusive licensing deals with third-party

content providers for software and content to be available only on a specific wireless carrier's network and wireless device[8]. In such cases the carrier, as an exclusive licensee, also becomes a "copyright owner" under the explicit terms of the Copyright Act. 17 U.S.C. § 101.

If a device from one carrier is unlocked and used on another network, that device may be preset to direct the user to content providers with whom the new network may not have a revenue sharing agreement. In such case, the carrier's network resources would be burdened with a higher percentage of downloads, but without the relevant revenue, while the customer's access to content supported by his or her carrier might be restricted by the absence of appropriate software.

In addition, many other copyrighted works, such as the software for instant messaging, multimedia messaging, browsing, video streaming, and network gaming, require that the phone contain specific carrier settings. These settings authenticate access to servers that complement the applicable client software (often carrier-customized) on the device. A device being operated on the wrong carrier will likely not be able to reach those servers, and high-value applications may not function. If the device reaches a similar server on the new network, the customized client software or settings may not be compatible.

For reasons such as these, to exempt circumventions, in order to allow customers to move phones freely to alternate networks, may restrain technological expansion in the hardware and software products and services that wireless carriers develop and market. Growth in making copyrighted content available through carriers would be impaired by allowing phones to be switched between carriers in that manner; and carriers would not be able to provide so many

[8] Most copyrighted content available through wireless devices, however, is widely available to users through marketing channels other than wireless carriers.

consumer choices in the customized qualities of a particular carrier offering of network, software, device and content.

In the current market system, the dissemination of copyrighted materials by wireless devices for non-infringing uses has been increasing at a fast rate, and there is no indication that current access control measures hinder that access. On the contrary, the technological measures now in place have facilitated such dissemination, and have substantially enhanced the availability of copyrighted works for such uses, through the many different permutations and combinations of business models that such measures permit.

Carriers also often subsidize downloads to wireless devices, in the expectation that they will recoup that investment. Exempting circumvention of technological measures would make it less likely that a carrier would be able to recoup its investment in the phone and in the downloaded content, would discourage the dissemination of innovative content and applications, and potentially would raise prices.

The current market has greatly fostered the American consumer's access to downloadable copyrighted content. In 2005, musical content sold in mobile formats such as ringtones, ringbacks and other artist-related content, represented $421.6 million in retail value. *See* http://www.riaa.com/news%5Cnewsletter%5C033106.asp. BMI, which tracks such sales, has projected that ringtones will generate $600 million in sales in 2006, up from $500 million in 2005, $245 million in 2004 and $68 million in 2003. *See* BMI release at http://www.bmi.com/news/200604/20060403a.asp. Millions of wireless subscribers also download mobile games, and mobile video (and mobile television). These offerings are proliferating with various types of content available from multiple carriers.

Copyright owners and their licensees do not authorize users of their works through wireless systems for those who are not legitimately authenticated by the carriers' access control measures. Those users who are not so authenticated are infringing users - - and infringers who do not pay the copyright owners and licensees for their uses. Such infringing uses will significantly impair the value of the works for the copyright owners in the burgeoning wireless market.

Software locks effectively control access to the integrated handset systems, network software, and content used by wireless carriers. Other measures, such as digital rights management (DRM), would not sufficiently protect against unauthorized access to the copyrighted content software beyond the scope of the license granted by the content provider and wireless carrier. For some carriers, many of the current content download license agreements restrict transfer of the application to someone other than the licensee. DRM protects against unauthorized copying of the work from a licensed device/media to an unlicensed device/media, and against playing the content on the licensed device after it ceases being a licensed device (*e.g.*, after the subscription term has ended).

In some configurations, DRM may check only to determine if the device has been authenticated to receive the content, and if the initial access control measure has been defeated or circumvented, some copyrighted content may be accessible without further restriction. Only broader access control methods, such as software locks, protect against unauthorized use of the downloaded content on another network, such as the use of ringtones and games on the licensed device by a transferee of that device (*e.g.*, one to whom a used device is resold) or by one who stole the phone from the original user and then tries to use it.

(3) What information, process or treatment must be applied in order to gain access to that copyrighted work(s) (or the identified portion(s) of the work(s)).

As described earlier, gaining authorized access to make noninfringing uses of any of the copyrighted works may require use of a variety of forms of information, processes or treatments. For example, under the technological measure in the SIM process, to access either the copyrighted works that are on the handset or the copyrighted works on the wireless network, codes must be matched between the network and the SIM card.

When the matching requirement is avoided, bypassed, removed or otherwise circumvented, the software does not perform the initial code matching operation that is prerequisite to authorized access to the network and content software on the handset, as well as to the copyright content on the network. Circumventing these access controls by deactivating the lock, adapts the software on the phone to create a new unauthorized "unlocked" version of handset software. Aside from the infringing use of the operating system in the handset software, circumvention of the software locks would create the possibility of a panoply of infringements of other content either on the handset or on the network. 17 U.S.C. §§ 106(1) through 106(6).

(4) In what respect is access to that copyrighted work controlled by the software lock, including (but not confined to): (a) what is the nature of the access to the copyrighted work that is controlled by the software lock?

The nature of the access is that it is specific authorization for an identified and authenticated person to use the handset and the wireless network, which in turn permits access to copyrighted network and content software.

(5) How does the software lock control such access to the copyrighted work?

(Please see our response to question number 1.)

(6) Describe whether and how the authority of the copyright owner of the copyrighted work is implicated in the operation of the software lock, including (but not confined to):

(a) who (e.g., the firmware manufacturer, the handset manufacturer, or the telecommunications service provider) installs and/or activates the software locks on the cellular phone handsets;

(b) whether the software locks are applied "with the authority of the copyright owner," and

(c) if the software locks are not installed by the copyright owner,

i. **what is the relationship between the copyright owner and the person who installs the software locks;**

ii. **are (and if so, in what respect are) the software locks applied with the permission of the copyright owner;**

(d) In what respect has the copyright owner authorized the application of information, or a process or a treatment, to gain access to the work.

In most cases, the handset manufacturer installs and activates these technological measures as agreed with the carrier. Where the copyrighted works are not owned by the manufacturer or the carrier, they are licensed to them directly or indirectly by the copyright owners for use only as authorized by the carrier and copyright owner.[9]

For copyrighted works owned by the handset manufacturers and/or the wireless carrier, they have the necessary authority as owners. The licensing terms for third-party copyrighted

[9] Of course, as already indicated, *see* answer to Question No. 2(a) above, in those instances where the licensee is an exclusive licensee, the licensee itself is a "copyright owner" under 17 U.S.C. § 101.

works are often highly negotiated, and typically include strict limitations. These limitations may permit sublicensing of certain use rights solely to a particular wireless carrier's subscribers, and require the carrier to implement technological measures to limit use as prescribed by the copyright owner. A third-party copyright owner typically will also impose confidentiality terms, requiring a handset manufacturer/vendor or a wireless carrier to protect confidential and proprietary information, which may include the content of certain copyrighted works.

For copyrighted works that the carrier owns, the relationship between the carrier and the party installing the access control measure (*i.e.,* a handset manufacturer/vendor) is typically contractual, with its installation expressly or impliedly authorized by the carrier.

For copyrighted works owned by a party other than the manufacturer/vendor or the carrier, the typical relationship is also contractual between the copyright owner and the manufacturer/vendor installing the access control measure: the copyright owner has licensed the copyrighted materials to the manufacturer/vendor. If the copyright owner has licensed the copyrighted materials to a wireless carrier, the manufacturer/vendor installing the access control measure may be a party to the licensing agreement and thereby authorized to install the measure, or impliedly authorized to do so when the copyright owner has knowledge of a carrier's practices or requires such measures as a condition to licensing the copyright content.

The copyright license requires the licensee to pay for uses that it permits consumers to make, and may also require the licensee to restrict access to the works in ways that will minimize infringing uses: whether enabled by circumvention of technological measures or otherwise, infringing uses are unpaid uses that impair the value of the copyrighted works.

In all respects, the access control measures are installed, activated and applied with the

authority of the respective copyright owners; and those copyright owners have in all respects authorized the use of the measures necessary to effectively control access to their works.

(7) In what circumstances, if any, is access to the copyrighted work authorized by the copyright owner

As indicated above, the copyright owner authorizes access to the copyrighted work only in those circumstances necessary for the noninfringing uses of the work that the owner permits at each stage by the manufacturer, the carrier, and ultimately by the authorized consumer.

These access controls allow a carrier or handset manufacturer to better maintain the quality of service associated with its products, network and brand identity. Maintaining a high level of service quality is a further circumstance for restricting authorized access. Customers are highly sensitive to service quality, and may terminate service with a carrier due to perceived deficiencies in the carrier's services.

Service problems experienced by subscribers may be attributable to, among other factors, handsets, the network, or incompatibilities between the two. From the customer's perspective, the source of the problem may be difficult to identify, and problems may well result in dissatisfaction with the wireless manufacturer, the wireless carrier, the content provider, or some combination of these entities. Carriers must therefore adopt policies and practices designed to ensure that customers will receive a high quality of service.

To maintain service quality, and to preserve their reputation, carriers must extensively test and evaluate various handsets under the specific conditions of their own networks, before authorizing their activation on their network. Carriers strive to maximize the efficiency of their networks; and handsets not designed for their networks may decrease network efficiency, result

in poor performance for a customer, or degrade service to other customers. A carrier's ability to decline authorization for activating certain handsets enables the carrier to maintain the quality of service it provides to subscribers, and thus to maintain the carrier's reputation.

From the trademark and service mark standpoint of maintaining their "brands," both handset manufacturers and carriers must be able -- for both legal and practical reasons -- to control the nature and quality of the goods and services that are identified under their brands when provided to the consumer. And maintaining the viability of the access control measures thus also facilitates the delivery of quality goods and services to the consumer.

(8) Whether the software locks in question are technological measures that "effectively control access to a work" as defined in §1201(a)(3)(B)

As shown above, the software locks in question are technological measures that "effectively control access" to myriad copyrighted works on wireless handset devices and networks, as defined in §1201(a)(3)(b).

Indeed, it is precisely because of the ability to control access effectively that the wireless industry has been able to make available to consumers wireless handsets that make available a plethora of works such as music, videogames, audio-visual materials, text, graphics, computer programs and other copyrighted content for noninfringing uses. It is not clear how the proposed exemption would enable the making of noninfringing uses -- a clear statutory prerequisite for the consideration of any such exemption, 17 U.S.C. § 1201(a)(1)(c), -- when the copyright owners who have declined to authorize access will presumably decline also to give the authorization necessary to convert infringing uses of their works into noninfringing uses.

Reprogramming a wireless phone to work on a different carrier's network is essentially modifying the code and creating an unauthorized derivative work -- an infringing act, not a

noninfringing use. The various software locks effectively control access to that code, and therefore the DMCA protects such access control measures.

The software access controls for wireless handsets provide the same benefits to consumers and creators of copyrighted works that access controls such as CSS, which allowed similar burgeoning of legitimate channels of distribution for DVDs. Enforcing software access controls further promotes the widespread availability of copyrighted works, and specifically those made available through wireless devices. Proposers have not put forth any reason sufficient to grant an exception.

D. FURTHER INFORMATION SHOWING WHY THE EXEMPTION SHOULD NOT BE GRANTED

Robust Competition In The Wireless Industry Benefits Consumers

Software locks enable wireless carriers to "bundle" discounted handsets with their wireless service. Because both the handset market and the market for wireless services are so competitive, consumers benefit from these bundles. It is widely acknowledged that the market for wireless services allows consumers to benefit from "robust competition." *In re Wireless Tel. Servs. Antitrust Litig.*, 385 F. Supp. 2d 403, 412 (S.D.N.Y. 2005); *see also* In the Matter of Bundling of Cellular Customer Premises Equipment and Cellular Service, 1992 WL 689944, 7 F.C.C.R. 4028 (F.C.C. June 10, 1992)(NO. FCC 92-207, CC 91-34). The exemption proposal fails to explain why this robust competition does not provide a competitive answer to the proposer's concern in the marketplace of a free economy.

This competitive marketplace has driven carriers to adopt different policies including "'varying pricing levels and structures, for varying service packages, with various available handsets and policies on handset pricing,'" *In re Wireless*, 385 F.Supp.2d at 412 (quoting 2003

findings of the FCC), and "'lower prices to consumers and increased diversity of service offerings.'" *Id.* (quoting 2000 findings of the FCC).

Contrary to the proposer's assertion to the Copyright Office in this proceeding that consumers have been impeded from accessing other wireless carriers' networks, Proposer's Comments at III(F), wireless carriers lose between 18 and 36 percent of their respective customers each year, *id.*, and presumably a significant portion of the customers switch to another carrier. Due to the widespread availability of discounted handsets "bundled" with the provision of service to new customers, handset locks are not a barrier to customers changing wireless carriers.

Again contrary to an assertion by the proposer (that the FCC, let alone Congress, "explicitly rejected" the carriers' practice of bundling the device with the carrier's service, Proposer Comments at III(F)), the FCC's 1992 Report and Order concluded that:

> [T]here is a robust level of competition that exists in the [wireless device] markets notwithstanding the common practice of packaging [wireless devices] and cellular service. This marketing practice of packaging [wireless devices] and cellular service has existed for several years and has benefited consumers.

Report and Order of the FCC, FCC Record No. 13, ¶ 14, FCC 92-207. The FCC also held that allowing carriers to bundle the devices with their networks "furthers the Commission's goal of universal availability and affordability of cellular service and thus promotes the continued growth of the cellular industry." *Id.* ¶ 20. Accordingly, the FCC specifically acknowledged that its policy decision to allow the practice benefited the American consumer as well as the cellular services market. *Id.*

And still again contrary to an assertion in proposer's comments (*i.e.*, that "almost every carrier today forces customers to purchase handsets directly from the carrier or its approved agent," Proposer's Comments at III(B)(1)(a)), consumers are offered a wide variety of policies

with regard to software access controls. At least one carrier does not require that most handsets it sells remain locked throughout the term of the customer's service agreement. Rather, for a customer making an unlock request, it will unlock most handsets that it sells, if the customer has maintained his or her account for at least 90 days and the account is fully paid at the time of the unlock request.

Indeed, if consumers wish, they can purchase phones that do not implement software locks. Consumers may purchase unlocked phones from various retailers and other parties, and many carriers permit use and operation of those phones on their networks. In the marketplace for wireless service, many carriers remain willing to activate devices that are not purchased from them, so long as the carrier has approved that type of device for use on its network and the device supports Enhanced 911 calling features. Such handsets are typically not offered at reduced rates, however, and so most consumers choose to purchase a handset that is locked to a particular carrier.

Proposer does acknowledge that, after evaluation, the FCC found that factors contributing to the competition in the market "were low barriers to entry . . ., a wide selection of handsets from which customers could chose, no evidence that carriers were refusing service to customers that purchased other brands of handsets, and a geographically fragmented market." Proposer Comments at III(B)(1)(a). These factors are even more evident in the wireless market today.

The ability of the carriers to maintain software access controls has also led to the creation of innovative new copyrighted works in software residing on the handset. In its recent decision in *In re Wireless Tel. Servs. Antitrust Litig.*, 385 F. Supp. 2d 403, 430-31 nn. 40 and 41 (S.D.N.Y 2005), the court found not only no showing that software locking had any anti-competitive effect, but also that locking has incentivized handset innovations and has facilitated the wider

availability of new products to consumers, by using new handsets to bring new customers to different wireless providers. *Id.* at 430, nn. 40 and 41. Handset manufactures reply on software access controls for allowing innovative handsets to be widely distributed through carrier subsidies.

Today, there are many more companies producing wireless devices, and the spectrum of types of devices has increased exponentially. There is no indication that the market for handset manufacturing is impaired – quite the contrary, it is thriving. And, as the court concluded, this practice has assisted innovations and widespread availability in the handset market. *Id. and accompanying text.*

The choice of carriers for the average consumer has also increased dramatically. In 1992, there were usually only two carriers in any given market for an individual consumer to choose among. Today, the vast majority of American consumers can choose among four, five or more carriers. *Id.* at 412. The FCC repeatedly has found in its annual reports to Congress on the state of competition in the wireless industry that the industry is competitive. Among the indicators of market structure that support this conclusion, the FCC noted that 97 percent of the total U.S. population lives in counties with access to three or more different operators offering mobile telephone service, up from 88 percent in 2000. *See Tenth Report*, In the Matter of Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, Annual Report and Analysis of Competitive Market Conditions With Respect to Commercial Mobile Services, 2005 WL 2428465, WT Docket No. 05-71, FCC 05-173, released Sept. 30, 2005, ¶ 2; *see also id.* ¶ 95 (there is effective competition in rural areas).

Between 2000 and 2005, the proportion of the U.S. population with four or more commercial mobile radio service (wireless) providers offering service in their counties grew from 79.8 percent to 93.2 percent, and the proportion with five or more grew from 68.5 percent to 87.3 percent. *See* Implementation of Section 6002(b) of the Omnibus Budget Reconciliation Act of 1993, 2005 WL 2429714, 20 F.C.C.R. 15,908 (F.C.C. Sep. 30, 2005) (NO. 05-71, FCC 05-173). In 2004, for the first time, there were more wireless subscribers than wireline access lines, due to the "relatively low cost, widespread availability, and increased use of wireless service." *Id.* at 15980.

The cellular service component of the Consumer Price Index (CPI) has *declined* more than twelve percent since 2000, while the overall CPI has *increased* over nine percent. *See id.* at 15995. The average cellular revenue per minute has been cut in half since 2000. *See id.* at 15996.

Proposers concede that as of 2005, 95% of new subscribers had a choice among multiple major carriers. Granting the exemption would restrict the needed flexibility of the wireless industry in determining the business models that would best facilitate the dissemination of entertainment software and other consumer software through the use of wireless devices. More and more, the "handset" is being expanded in the wireless industry to encompass the complex devices previously described; and their further development would be significantly impaired by the proposal. It is not an overstatement to conclude that the proposed change would threaten to undermine the market forces that promote innovation and competitive benefits for consumers nationwide.

The Copyright Office Is Not the Appropriate Forum for Proposals to Restructure the Wireless Industry

The Wireless Alliance basically seeks to restructure the wireless industry in a way that it contends will increase competition. Even assuming that the exemption would achieve such a result -- and it would not - - CTIA respectfully submits that the Copyright Office is the wrong forum to determine any such restructuring.

The FCC is the agency primarily responsible for the regulation of radio transmissions and services. The Communications Act of 1934, as amended (the "Communications Act"), designates the FCC as the "centraliz[ed] authority" responsible for "execut[ing] and enforc[ing]" federal communications policies.[10] As the Supreme Court has recognized, the Communications Act provides the FCC with "comprehensive powers to promote and realize the vast potentialities of radio."[11] The FCC is responsible for "licensing and regulating" the broadcast spectrum,[12] and has the power to "[p]rescribe the nature of the service to be rendered by each class of licensed stations,"[13] "encourage the larger and more effective use of radio in the public interest,"[14] and, generally, to "[m]ake such rules and regulations . . . as may be necessary to carry out the provisions of this [Act]."[15]

---

[10] 47 U.S.C. § 151.

[11] *NBC v. United States*, 319 U.S. 190, 217 (1943).

[12] 47 U.S.C. § 152(a).

[13] *Id.* § 303(b).

[14] *Id.* § 303(g).

[15] *Id.* § 303(r). *See id.* § 154(i) (authorizing the FCC to "perform any and all acts, make such rules and regulations, and issue such orders, not inconsistent with this [Act], as may be necessary"). *See also FCC v. Midwest Video Corp.*, 440 U.S. 689, 706 (1979) (explaining that

"The Communications Act was implemented for the purpose of consolidating federal authority over communications in a single agency to assure an adequate communication system for this country."[16] In light of the FCC's broad experience and knowledge of the wireless industry, and the express rulemaking power that Congress has vested in the FCC, the Copyright Office should defer to the expert agency's repeated determinations that consumers benefit from handset bundling and the wireless industry's competitive structure. If there is a structural issue that impedes competition in the wireless industry, it is the FCC, not the Copyright Office, that should address it.

Nor is the Copyright Office the proper forum to address the environmental concerns expressed by the proposer. The wireless industry already has a robust recycling program, including CTIA's *Wireless... The New Recyclable* program. *See* www.recyclewirelessphones.com. Although it may be the proposer's experience that "phones that are not locked to a specific carrier are much easier to recycle and sell",[17] there is no indication that access control measures prevent the proposer from the proper performance of

---

the FCC's regulatory authority includes any actions "necessary to ensure the achievement of the Commission's statutory responsibilities").

[16] *See Motion Picture Ass'n of Am. v. FCC*, 309 F.3d 796, 804 (D.C. Cir. 2002); *Sprint Spectrum L.P. v. Mills*, 283 F.3d 404, 416 (2d Cir. 2002) ("As we recently discussed . . . the [Communications Act] was designed 'to "centraliz[e] authority heretofore granted by law to several agencies" in the FCC, and to "grant[] additional authority with respect to interstate and foreign commerce in wire and radio communication" to the FCC.' . . . We found that '[t]hese statutory provisions make it clear that Congress intended the FCC to possess exclusive authority over technical matters related to radio broadcasting,'" (quoting *Freeman v. Burlington Broadcasters, Inc.*, 204 F.3d 311, 320 (2d Cir. 2000) (quoting 47 U.S.C. § 151)).

[17] Digital Millennium Copyright Act, 1201(a)(1) Rulemaking: Public Hearing on Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies before the United States Copyright Office, 37 CFR Part 201, Docket No. RM 2005-11, at 7 (2006) (statement of Jennifer Stisa Granick, The Wireless Alliance).

recycling activities.

E. CONCLUSION

The information set forth above demonstrates that The Wireless Alliance has not met its burdens of proof under Sec. 1201(a)(1)(A), let alone its burden of proof to show that rulemaking in the Copyright Office is the proper forum for consideration of its proposal.

September 11, 2006

COWAN, LIEBOWITZ & LATMAN, P.C.

Morton David Goldberg
mdg@cll.com

Jason D. Sanders
jds@cll.com

1133 Avenue of the Americas
New York, NY 10036-6799
(212) 790-9200

Attorneys for CTIA – The Wireless Association®

Of counsel:

Michael F. Altschul
Senior Vice President and General Counsel
CTIA-The Wireless Association®
1400 16th Street, NW Suite 600
Washington, DC 20036