

Cowan, Liebowitz & Latman, P.C.

Law Offices

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

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

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

September 22, 2006

David O. Carson, Esq.
General Counsel
United States Copyright Office
Copyright GC/I&R
P.O. Box 70400
Southwest Station
Washington, D.C. 20024-0400
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:

On behalf of CTIA – The Wireless Association®, we write in response to your September 18, 2006 letter, which asked for further information to support the submission of our answers of September 11, 2006 to the questions posed in the Office letter of August 14, 2006 to Ms. Granick and Mr. Metalitz. Enclosed please find a more formal petition for consideration of our September 11, 2006 submission.

We are delivering 15 copies of this petition through the United States Postal Service to the above address stated in the Notice of Inquiry. We are also delivering a courtesy copy by hand addressed to you at the United States Copyright Office, James Madison Memorial Building,

Cowan, Liebowitz & Latman, P.C.

David O. Carson, Esq.

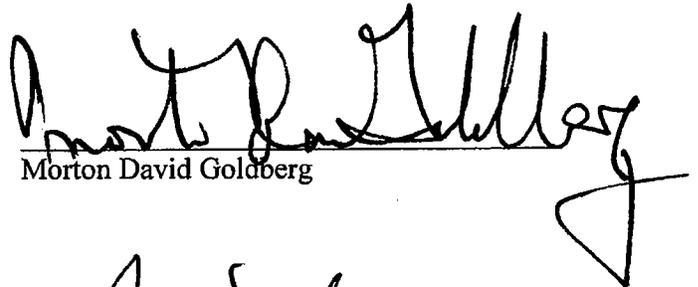
September 22, 2006

Page 2

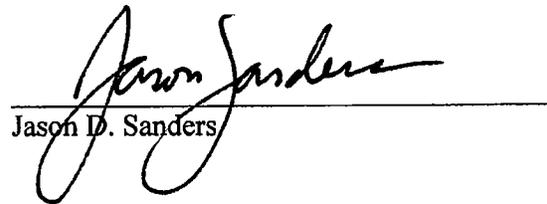
101 Independence Avenue, SE, Washington, D.C. 20559-6000,¹ as well as electronically to your email address listed above.

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

Lance D. Reich, Esq.
One Atlantic Center
1201 W. Peachtree Street, Suite 3000
Atlanta, Georgia 30309
ldreich@carltonfields.com

¹ On September 11, 2006, we delivered 15 copies of the September 11 submission by hand to you at the Madison Building address, in the belief that delivery to that address would be the most expeditious for the hard copies.

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

Petition Submitted
on Behalf of

CTIA – THE WIRELESS ASSOCIATION®

Petition for Consideration of Its “Complementing Response to Copyright
Office Request of August 14, 2006 for Further Information,”
Submitted on September 11, 2006

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

Table of Contents

I.	INTRODUCTION AND SUMMARY	1
II.	CTIA REPRESENTS THE WIRELESS INDUSTRY	3
III.	CTIA’S DELAY WAS NOT UNREASONABLE.....	4
	A. CTIA Received Initial Notice In January or February.....	4
	B. CTIA Has Proceeded With Great Diligence Since August	6
IV.	THE COPYRIGHT OFFICE SHOULD GIVE CONSIDERATION TO THE CTIA SUBMISSION	7
	A. With Only A Short Time For The Evaluation To Be Made, The Record is Admittedly Thin And More Information Is Required to Complete it.....	7
	B. Both Witnesses Acknowledge That They Lack The Information Sought, But That CTIA And Its Members Do Possess The Information.....	8
	C. The Information Will Significantly Affect the Register’s Recommendation	10
V.	CONCLUSION.....	11

Exhibit A – August 14, 2006 letter of David O. Carson to Jennifer Granick and Steven Metalitz

Exhibit B – September 11, 2006 letter from Morton David Goldberg and Jason D. Sanders to David O. Carson, attaching CTIA’s September 11, 2006 Submission to the Copyright Office

Exhibit C – September 11, 2006 Submission by CTIA to the Copyright Office, Complementing Response to Copyright Office Request of August 14, 2006 for Further Information

Exhibit D – September 11, 2006 letter of Steven J. Metalitz to David O. Carson

Exhibit E – September 11, 2006 Response to Supplemental Questions of the Copyright Office, by The Wireless Alliance and Robert Pinkerton [Exhibits thereto omitted herein]

Exhibit F – September 18, 2006 letter of David O. Carson to Morton David Goldberg

Exhibit G – September 18, 2006 letter of David O. Carson to Jennifer Granick

I. INTRODUCTION AND SUMMARY

CTIA – The Wireless Association® (“CTIA”) submits this Petition for Consideration of its “Complementing Response to Copyright Office Request of August 14, 2006 for Further Information,”¹ which CTIA submitted to the Office on September 11, 2006,² regarding the proposed exemption for “Computer programs that operate wireless communications handsets”; and CTIA submits this Petition in response to the Office letter of September 18, 2006,³ which asked for further information to justify consideration of CTIA’s submission.⁴

In its September 11 submission and cover letter, CTIA described how it learned of the Copyright Office’s request for further information regarding wireless communications handset technology and the related copyrighted works, and provided information essential to an accurate evaluation of the proposal. To any extent that CTIA’s September 11 submission and letter may not have fully addressed the Office requirements, this petition will provide further information

¹ CTIA’s submission was intended to complement the response of September 11, 2006 by Steven J. Metalitz (Exhibit D hereto) to the Copyright Office request of August 14, 2006 (Exhibit A hereto) for detailed information the Office needed to complete its evaluation of the proposed exemption. CTIA spoke only for its members, not for Mr. Metalitz’s clients.

² CTIA’s September 11 submission is Exhibit C hereto; and the cover letter of that date from Morton David Goldberg and Jason D. Sanders to David O. Carson is Exhibit B hereto.

³ Letter of September 18, 2006 from David O. Carson, General Counsel of the Office, to Morton David Goldberg, of Cowan, Liebowitz & Latman, P.C., counsel for CTIA in this proceeding, (Exhibit F hereto).

⁴ Mr. Carson’s letter to Mr. Goldberg (Exhibit F hereto), stated that CTIA’s September 11, 2006 submission did not appear to comply with the Notice of Inquiry requirements that, *inter alia*, CTIA state why the information was not provided earlier and why it should be considered after the deadline for comments.

that justifies Office consideration of CTIA's submission, including an explanation of the timing in making the submission and the reasons why the submission should be considered notwithstanding any delay in its submission.

CTIA believes that its submission should be considered by the Copyright Office. As the Office itself has acknowledged, even after the hearing on questions concerning the proposal, "the record on these questions is rather thin and we require more detailed information in order to complete our evaluation of the proposed exemption."⁵

CTIA's submission provides the detailed technological and business information necessary for the Office to complete its evaluation. It provides explanations of the various access control measures used by the manufacturers and carriers, and of the various layers of content to which access is effectively controlled, including handset operating systems, applications and additional content such as photographs and music, as well as critical information regarding the significant continuing integration of these types of software.

The submission also provides the Office with essential information regarding the ownership and licensing of the copyrighted works on the handsets, the growing use of exclusive licensing arrangements, and the technological issues that impact the use of copyrighted works if handsets are switched between carriers. Other benefits of software locking are described, such as protection against theft and fraud, and how carriers are enabled thereby to subsidize the cost of the handset, especially in the context of "pre-paid" wireless plans.

⁵ Letter of August 14, 2006 from David O. Carson to Jennifer Granick and Steven Metalitz (Exhibit A hereto), at 2.

The submission also clarifies the record regarding the claimed need for an exemption to permit the circumvention of the access controls, by supplying the information that some carriers do not lock their handsets and others unlock the handset at the customer's request. And CTIA's submission also provides the necessary broader market context, such as the declining cost to the consumer of wireless service, the increased choice of carriers for the consumer, and that the FCC has repeatedly found the wireless market to be competitive.

Because of its broad membership across the wireless industry, CTIA's submission provides the detailed information needed by the Office, information that the Office would not have otherwise.

As a summary of the submission makes clear, CTIA firmly believes that consideration of the submission would significantly affect the Register's recommendation as to the proposed exemption.

II. CTIA REPRESENTS THE WIRELESS INDUSTRY

As stated more fully in CTIA's submission, CTIA is a non-profit trade association of the wireless industry, representing both wireless carriers and manufacturers. CTIA's membership serves over 95% of the more than 224 million wireless customers in the United States, and includes the major suppliers of the handsets used by wireless subscribers to access wireless networks. This breadth of membership allows CTIA to draw upon a wide range of knowledge of both the technological and business aspects of the wireless communication industry, including the wide range of content, technology and applications provided by wireless carriers and others in the wireless "ecosystem." Accordingly, CTIA is particularly well-situated to provide the Copyright Office with information bearing upon its evaluation of the exemption proposal.

III. CTIA'S DELAY WAS NOT UNREASONABLE

A. CTIA Received Initial Notice In January or February

In the Office's September 18 request for further information regarding the reasons for CTIA's submission after the deadline for Reply Comments, it has asked three specific questions, which we have put to CTIA, and which we can now answer as follows:

1. When did CTIA – The Wireless Association first become aware of:
 - A. The current rulemaking proceeding; and
 - B. The fact that the exemption upon which you now seek to comment was being sought?

CTIA first became aware of the current rulemaking proceeding, and the fact that an exemption for "Computer programs that operate wireless communications handsets. (Mobile firmware)"⁶ was being sought, either in early February 2006 or at the very end of January 2006.

⁶ The quoted phrasing of the proposed exemption appears in the proposer's original submission and in Mr. Carson's letter of September 18, 2006 to CTIA's counsel (Exhibit F hereto), at 1. The proposer's Reply Comments describe a slightly different proposal, one to exempt "Computer programs that operate a mobile phone handset. (Mobile firmware)." CTIA does not know which of the two proposals it became aware of in the period described above.

It was concerning a third proposal, however, that CTIA submitted its information in answer to the questions in the Office letter of August 14, 2006 (Exhibit A hereto), at 1. That proposal was, in the letter's description, a proposal to exempt "Computer programs that operate wireless communications handsets."

A fourth and fifth proposal are found in the proposer's September 11, 2006 Response to Supplemental Questions of the Copyright Office from The Wireless Alliance and Robert Pinkerton (Exhibit E hereto), at 10: "an exemption that allows circumvention of any software lock that controls access to any part of mobile firmware required to operate the handset on the network of the user's choice"; and at 13: an exemption for "computer programs that enable wireless telecommunications handsets to connect to a wireless communication network."

2. Did any members of CTIA – The Wireless Association become aware of –
 - A. The current rulemaking proceeding; or
 - B. The fact that the exemption upon which you now seek to comment was being sought,

-- prior to the time identified in response to question 1?

CTIA has no knowledge that any members of CTIA became aware of the current rulemaking proceeding or became aware of the fact that the exemption was being sought for “Computer programs that operate wireless communications handsets. (Mobile firmware)” -- or, for that matter, any of the other varying proposals for exemption⁷ -- prior to the time identified in response to question 1.

3. If the answer to question number 2 is “yes,” please:
 - A. Identify the member or members of CTIA – The Wireless Association in question;
 - B. State what information the member or members became aware of and when the member or members became aware of that information.

In light of the response to question 2, this question is not applicable.

CTIA represents more than 200 companies, and those companies employ an aggregate of hundreds of thousands of persons. In answering questions 2 and 3, CTIA speaks only of its knowledge as to any awareness of members in the relevant period; and, as stated above, it has no knowledge of any such awareness. At no time has any CTIA member brought to CTIA’s attention the current rulemaking proceeding or the fact that the varying exemption proposals were being put forward.

⁷ See preceding footnote.

When CTIA first became aware of the rulemaking proceeding, CTIA passed the information on to a select group of member contacts; and, in retrospect, these contacts may not have been the correct group to address this issue. After that initial forwarding of the information, CTIA received no further information regarding this rulemaking, made no plans to participate in this proceeding, and was not aware until August 2006 of any events in the ongoing proceeding or that the Office required any additional information to evaluate whether the proposal had any merit.

B. CTIA Has Proceeded With Great Diligence Since August

Last month, in August, CTIA again became aware of the proceeding. About the same time, it also became aware that on August 17, 2006, the United States government had filed a criminal complaint asserting §1201 anti-circumvention violations in an effort to stem wireless handset fraud,⁸ and that the proposer was misrepresenting on its website that CTIA was a “partner” in proposer’s recycling business.⁹ CTIA raised the exemption issue promptly with the general counsels at several of the carriers, informing them that the Copyright Office was now proceeding to make a recommendation concerning an issue on which they had important and relevant information that the Office needed.

⁸ In United States v. Othman, No. 06-MJ-30401, filed in the United States District Court for the Eastern District of Michigan, the government alleged 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. §§1201(a)(1)(A) and 1204(a), in order to sell them at market (non-subsidized) prices outside of the United States. The complaint was dismissed on September 7, 2006.

⁹ As indicated below, at page 10, the misrepresentation as to the claimed partnership of the proposer was not removed until after CTIA sent the proposer a cease and desist letter.

From that point until its submission on September 11, 2006, CTIA, its members and its counsel in this proceeding (who were retained on August 30, 2006) have acted speedily to gather and present the information relevant to answer the questions that the Office put in its August 14 letter, questions that presumably the Office deems necessary to be answered in order for it to make its recommendation on this issue. Put simply: Neither CTIA nor its members or counsel waited on the sidelines during the proceeding to “sandbag” the proposer or the proposal, or the Office or the public.

IV. THE COPYRIGHT OFFICE SHOULD GIVE CONSIDERATION TO THE CTIA SUBMISSION

The essential reasons why the Office should accept CTIA’s submission for consideration in evaluating the exemption proposal are that CTIA’s delay was not unreasonable in all the circumstances and:

- A. With only a short time for the evaluation to be made, the record is admittedly thin and more information is required to complete it;
- B. both witnesses acknowledge that they lack the information sought, but that CTIA and its members do possess the information; and
- C. the information will significantly affect the Register’s recommendation.

We give the basis for each of these further reasons in turn.

A. With Only a Short Time For The Evaluation To Be Made, The Record Is Admittedly Thin And More Information Is Required To Complete It

Sufficient information that the Office requires about highly technical facts and circumstances is not in the record. In its letter of August 14, 2006, the Office propounded numerous questions and sub-questions, and acknowledged that it required “more detailed

information in order to complete our evaluation of the proposed exemption.”¹⁰ It said the information was required because “the record on these questions is rather thin.”¹¹ Indeed, the Office need for clarifying technical information may be further accentuated by the additional uncertainty that has been generated by the varying descriptions used to define the exemption – or exemptions – being requested.¹²

Though the Office is “hopeful that we will be able to conclude this rulemaking proceeding by October 28 . . . ,”¹³ neither witness has been able to fully supply the information the Office requires. CTIA believes that CTIA’s response of September 11 provided what the Office required in its August 14, 2006 letter: accurate, well-founded answers to its detailed questions.

B. Both Witnesses Acknowledge That They Lack The Information Sought But That CTIA And Its Members Do Possess The Information

If the Office were not to consider the information that CTIA has provided, the Register would be making her recommendation without information that the Office has requested, and that it has said so clearly it must have. This circumstance is clear from the answers submitted both by counsel for the proposer,¹⁴ and by counsel for the Joint Reply Commenters.¹⁵ Those

¹⁰ August 14, 2006 letter of David O. Carson to Jennifer Granick and Steven Metalitz (Exhibit A hereto), at 2.

¹¹ *Ibid.*

¹² See Note 6 (at least five varying proposals have been described by the proposer).

¹³ September 18, 2006 letter of David O. Carson to Jennifer Granick (Exhibit G hereto), at 1.

¹⁴ See The Wireless Alliance submission of September 11, 2006 (Exhibit E hereto), at 3 (“More specific information in response to the Copyright Office’s questions is exclusively in the hands of the carriers and the handset makers”); *Id.* at 7 (“More detailed information than that provided may be entirely under the exclusive control of the phone makers and network providers”).

counsel were the only witnesses to whom the Office posed its questions on August 14, 2006. Each acknowledged -- with commendable candor -- that they did not have the requisite familiarity to supply more specific and detailed information about the technologies the Office had inquired about, but that the manufacturers and service providers did have that information, or that -- as indicated by Mr. Metalitz in his September 11 letter -- CTIA did, on behalf of those companies.

Indeed, Mr. Metalitz's response to the Office stated that "[w]e . . . encourage you to consider the new information contained in [CTIA's] submission which may be more responsive to your questions."¹⁶

CTIA represents the carriers and handset manufacturers that -- as proposer acknowledges -- have the unique ability to provide the necessary detailed information to the Copyright Office. CTIA has not sought to make a new proposal, nor to commence a new exemption proceeding or raise extraneous issues. Rather, it seeks to provide the information the Office requested in its letter of August 14, 2006, in order that CTIA may complement a record that the Office acknowledges requires such information.

¹⁵ See September 11 letter of Steven J. Metalitz to David O. Carson (Exhibit D hereto) at 1 ("As you state in your letter, the Joint Reply Commenters whom I represent do not include handset manufacturers, wireless carriers, or other telecommunications service providers. Thus, we have little information to provide in response to the specific questions posed in the letter. We understand that a separate submission may be made on behalf of CTIA - The Wireless Association, and encourage you to consider the new information contained in that submission which may be more responsive to your questions.").

Similarly, the August 14, 2006 letter of David O. Carson (Exhibit A hereto) acknowledged that Mr. Metalitz does not represent "handset manufacturers, telecommunications service providers or others directly involved [in] the activity that is the subject of the proposed exemption."

¹⁶ September 11 letter of Steven J. Metalitz to David O. Carson (Exhibit D hereto) at 1.

**C. The Information Will Significantly
Affect the Register's Recommendation**

CTIA has provided the information for consideration by the Office because the information will “significantly affect the Register’s recommendation.”¹⁷ As stated in our submission, we believe that the information submitted clearly demonstrates why the proposed exemption should not be granted.

Further, the proposer has relied upon the absence of any submission from CTIA’s members to suggest that -- contrary to fact -- those manufacturers and service providers have no objection to the proposed exemption.¹⁸ In addition, shortly before providing its comments, CTIA learned that The Wireless Alliance was listing CTIA as its “partner” in the proposer’s business of reselling used wireless devices, although there is no such relationship whatsoever. It was not until CTIA demanded that the proposer immediately cease and desist its misrepresentation that proposer deleted the “partnership” claim from its website.

As CTIA’s September 11, 2006 submission pointed out, neither the proposer’s statement of partnership with CTIA nor its statement of an implicit consent of CTIA’s members to its proposal has been accurate. Thus, CTIA believes it all the more important that the Office be fully informed of CTIA’s position on these issues, including the technological and business information uniquely in its possession on which its position is based.

¹⁷ See September 18, 2006 letter of David O. Carson to Morton David Goldberg (Exhibit F hereto), at 2; Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies (Notice of Inquiry), 70 Fed. Reg. 57526, 57531 (2005).

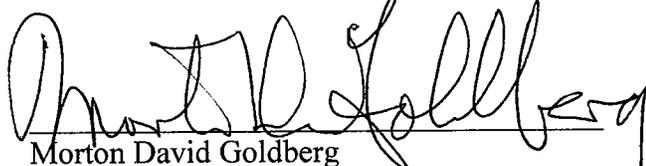
¹⁸ The Wireless Alliance September 11 Submission (Exhibit E hereto), at 3, 4 and 7.

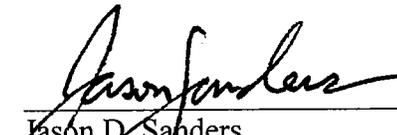
V. CONCLUSION

For the reasons stated, the Copyright Office should accept CTIA's submission for consideration and, on review, recommend to the Librarian of Congress that The Wireless Alliance has not met its burdens of proof under section 1201(a)(1)(C), let alone its burden of proof that rulemaking in the Copyright Office is the proper forum for consideration of its proposal.

September 22, 2006

COWAN, LIEBOWITZ & LATMAN, P.C.


Morton David Goldberg
mdg@cfl.com


Jason D. Sanders
jds@cfl.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

EXHIBIT A



The Register of Copyrights of the United States of America

United States Copyright Office · 101 Independence Avenue SE · Washington, DC 20559-6000 · (202) 707-8350

August 14, 2006

Jennifer Granick, Esq.
Stanford Law School Center for Internet & Society
Cyberlaw Clinic
559 Nathan Abbott Way
Stanford, CA 94305

Steven Metalitz, Esq.
Mitchell Silberberg & Knupp LLP
2300 M Street, N.W., Suite 800
Washington, D.C. 20037

Dear Ms. Granick and Mr. Metalitz:

I am writing to follow-up on your participation in the Copyright Office's March 23 public hearings of the DMCA Section 1201 Rulemaking relating to The Wireless Alliance's proposed exemption: "Computer programs that operate wireless communications handsets."

Having reviewed the record, we seek additional and more detailed information relating to whether the software locks described in the comments and testimony of The Wireless Alliance are technological measures that effectively control access to works protected under title 17, as defined in 17 U.S.C. §1201(a)(3)(B). Section 1201(a)(3)(B) provides:

a technological measure "effectively controls access to a work" if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.

Please provide us with any information you have relating to the following questions. Please provide the following information, separately for each of the four types of software locks described in the comments and testimony of the Wireless Alliance -- SPC locking, SOC locking, band order locking, and SIM locking:

- (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";
 - 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; and
 - 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.

To the extent that the answer to any of these questions varies depending upon the telecommunications service provider, handset manufacturer, handset model, firmware producer, or other parties who are involved, please provide explanations in your responses.

In addition to providing us with the requested information, we solicit your views on whether the software locks in question are technological measures that "effectively control access to a work" as defined in §1201(a)(3)(B).

We recognize that the comments and testimony of The Wireless Alliance have touched upon some of these questions, but the record on these questions is rather thin and we require more detailed information in order to complete our evaluation of the proposed exemption. We also recognize that Mr. Metalitz is not a proponent of the proposed exemption and does not represent handset manufacturers, telecommunications service providers or others directly involved the activity that is the subject of the proposed exemption. However, because it is our practice, when submitting questions to witnesses, to submit those questions to all persons who have testified on the proposed exemption, we wish to provide him with an opportunity to consider and respond to our questions.

Jennifer Granick, Esq.
Steven Metalitz, Esq.

Page 3

August 14, 2006

Because these questions have arisen at a fairly late point in this rulemaking proceeding, we would be grateful if we could receive your responses promptly, and in any event no later than August 28.

Thank you for your assistance in this rulemaking proceeding.

Sincerely,

A handwritten signature in black ink that reads "David O. Carson". The signature is written in a cursive style with a long horizontal flourish extending to the right.

David O. Carson
General Counsel

EXHIBIT B

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.

JOHN F. KENNEDY INTERNATIONAL AIRPORT OFFICE • JAPAN AIRLINES BUILDING 14, SUITE 11B • (718) 244-8595

27294/000/763157.2

Cowan, Liebowitz & Latman, P.C.

David O. Carson, Esq.

September 11, 2006

Page 2

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.

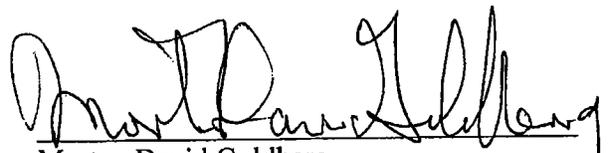
In submitting this information, CTIA of course speaks only for its members, not for Mr. Metalitz’s clients.

Cowan, Liebowitz & Latman, P.C.
David O. Carson, Esq.
September 11, 2006
Page 3

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

EXHIBIT C

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@ccl.com

Jason D. Sanders

jds@ccl.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 Inquiry¹, 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 contract 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).**

The Technological Measures Control Access to a Broad Spectrum of Copyrighted Works

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 device⁸. 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 rely 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).

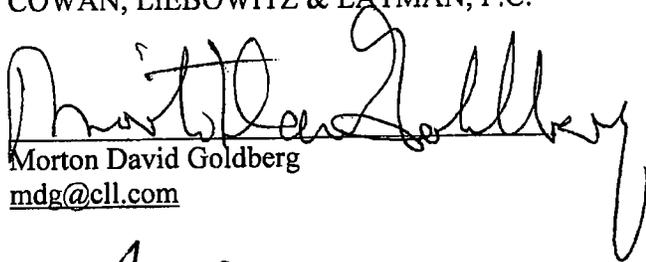
recycling activities.

E. CONCLUSION

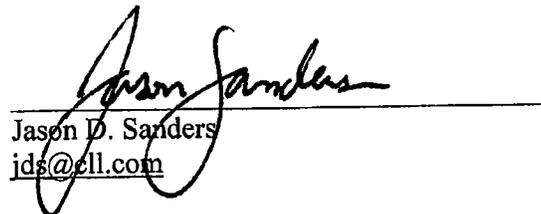
The information set forth above demonstrates that The Wireless Alliance has not met its burdens of proof under Sec. 1201(a)(1)(A), let alone its burden of proof to show that rulemaking in the Copyright Office is the proper forum for consideration of its proposal.

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

EXHIBIT D



Steven J. Metalitz
Partner
(202) 973-8136 Phone
(202) 973-8110 Fax
met@msk.com

September 11, 2006

VIA U.S. MAIL AND E-MAIL

David O. Carson
General Counsel
U. S. Copyright Office
Library of Congress
Copyright GC/INR
P. O. Box 70400
Southwest Station
Washington, DC 20024

Re: Response to August 14, 2006 Letter Regarding DMCA Rulemaking

Dear Mr. Carson:

The Joint Reply Commenters appreciate this opportunity to respond to your letter of August 14, 2006 regarding the proposed exemption: "Computer programs that operate wireless communications handsets." As you state in your letter, the Joint Reply Commenters whom I represent do not include handset manufacturers, wireless carriers, or other telecommunications service providers. Thus, we have little information to provide in response to the specific questions posed in the letter. We understand that a separate submission may be made on behalf of CTIA – The Wireless Association, and encourage you to consider the new information contained in that submission which may be more responsive to your questions.

With regard to question 2, which seeks information about the copyright works with respect to which access is controlled, we reiterate that in some circumstances these works would include not only the "mobile firmware" identified by the proponents of this exemption, but would also encompass many other works. These include music, sound recordings, audio-visual works, video games, literary works or photographs to which a user of the handset gains access in the form of ring tones, downloadable or streaming music, music videos or video clips, television series episodes, news/sports/weather reports, and a host of other content services that are increasingly integrated with subscriptions to wireless telecommunications services. See RC11 at 25-6 (raising concerns regarding the threat to content on wireless handsets that the exemption would create); see also Tr. at 15 (statement of Ms. Granick) (admitting that "some carriers may currently place DRM technology at the firmware level") and Tr. at 25 (statement of Mr.

Metalitz) (explaining that in cases where the handset lock and the DRM are “tightly integrated” this proposed exemption could have a substantial adverse impact on copyright owners).¹

We appreciate your consideration of this response and look forward to reviewing the submission of the proponents, and of the CTIA, in response to your letter. Please let me know if you have any further questions after review of those submissions.

Respectfully submitted,



Steven J. Metalitz
of
MITCHELL SILBERBERG & KNUPP LLP
2300 M STREET, NW, SUITE 800
WASHINGTON, DC 20037 USA
TEL: (202) 973-8136
FAX: (202) 973-8110
EMAIL: MET@MSK.COM

Counsel to Joint Reply Commenters:

AAP: Association of American Publishers
AAUMP: Association of American University Presses
ASMP: American Society of Media Photographers
The Authors Guild, Inc.
BSA: Business Software Alliance
DGA: Directors Guild of America
ESA: Entertainment Software Association
IFTA: Independent Film & Television Alliance
MPAA: Motion Picture Association of America
NMPA: National Music Publishers' Association
PPA: Professional Photographers of America
RIAA: Recording Industry Association of America
SAG: Screen Actors Guild
SIIA: Software and Information Industry Association

cc: Jennifer Granick

¹ For the purposes of this letter we refer to the Joint Reply Comments, which are available at http://www.copyright.gov/1201/2006/reply/11metalitz_AAP.pdf, as RC11. We refer to the official transcript of the Palo Alto hearing on March 23, 2006, which is available at <http://www.copyright.gov/1201/2006/hearings/transcript-mar23.pdf>, as Tr.

EXHIBIT E

Before the
Library of Congress Copyright Office
Notice of Inquiry *In re* Exemption to Prohibition on
Circumvention of Copyright Protection Systems for Access
Control Technologies

Response to Supplemental Questions of the Copyright Office

Submitted by:

Jonathan R. Newman
Vice President
The Wireless Alliance, LLC
5763 Arapahoe Road, Unit G
Boulder, CO 80303

Robert Pinkerton
909 N. Edgewood Street
Arlington, VA 22201

Represented by:

Jennifer Granick, Esq.
Stanford Law School
Center for Internet & Society
Cyberlaw Clinic
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-0014
(650) 723-4426 fax
jennifer @ law.stanford.edu

INTRODUCTION

Thank you for the opportunity to respond to the Copyright Office's questions in connection with our request for an exemption to section 1201(a). As you know, commentators submitted the initial request for the exemption, reply comments in favor of the exemption, and lengthy testimony in support of the exemption. Most of the post-hearing

questions for which the Copyright Office now requests responses for were answered in these submissions. In sum, mobile handset configuration, including locking, varies from model to model. Handsets are not much different from personal computers, except there are even more models and even more operating systems. Thus, it is impossible to completely catalog the locking mechanisms and to describe the configurations of every handset. Nonetheless, we have provided a large amount of both accurate and generally-applicable information that describes the way handsets work, and why section 1201(a) interferes with the non-infringing activity of unlocking.

By focusing on the technical details of mobile phone architecture, the Copyright Office implies that commentators must prove that section 1201(a) actually prohibits all phone unlocking. We need not. An exemption is based on a showing that the prohibition has or is likely to have a substantial adverse effect on non-infringing uses of a particular class of works. In order to meet the burden of proof, proponents of an exemption must provide evidence either that actual harm exists or that it is "likely" to occur in the ensuing three-year period.

The fact that the 1201(a) prohibition has been and continues to be used to challenge phone unlocking in the courts is overwhelming proof of actual harm. Since our testimony on March 23, 2006, phone carriers have filed multiple additional lawsuits claiming 1201(a) violations. Some of these defendants have had to settle the lawsuits, rather than incur expensive legal fees, and agree to stop unlocking. (See, TracFone Wireless, Inc. v. Pan Ocean Communications, Inc., et. al., United States District Court, Southern District of Florida, Case No. 05-61956-Civ (hereinafter Pan Ocean), Final Judgment and Permanent Injunction, Exhibit A; TracFone Wireless Inc. v. Clinton Riedeman d/b/a Larry's Cell, et. al., United States District Court, Middle District of Florida, Orlando Division, Case No. 6:06-CV-1257-ORL-18-JGG (hereinafter Larry's Cell), Complaint for Damages and Injunctive Relief, Exhibit B.) Additionally, TracFone recently emailed an unknown number of people in the secondhand handset business with misleading legal threats suggesting that TracFone and the FBI are working together to bring criminal charges against handset resellers. (True Copy of Email sent to Counsel for Commentators

by Phone Reseller Attached as Exhibit C) Counsel for commentators personally has received many phone calls from phone unlockers asking whether what they are doing is illegal. Any attorney receiving such a call would have to advise the client that it is difficult to say whether or not section 1201(a) applies to phone unlocking. As a result of this ongoing legal uncertainty, section 1201 further interferes with non-infringing activity. These showings are more than adequate to justify the exemption.

More specific technical information in response to the Copyright Office's questions is exclusively in the hands of the carriers and handset makers. Yet, these entities have not appeared to contest this request for an exemption or to provide the Copyright Office with additional information. Their failure to object does not diminish the fact that we have amply met our burden of proof.

Architecture variation poses no obstacle to granting this exemption. In some cases, section 1201(a) may not apply to phone locking, in some cases it may. Defendants in TracFone Wireless v. Sol Wireless, (United States District Court, Southern District of Florida, Case No. 05-23279-CIV, hereinafter Sol Wireless, attached as Exhibit D), Pan Ocean, Larry's Cell, and threatened resellers, recyclers and unlockers everywhere have no idea whether their practices violate the DMCA, for some or all models of handsets that they unlock. That is exactly why the public needs an exemption. The Copyright Office does no harm, and much good, in granting an exemption, even if the statute does not apply to all unlocking practices. If a particular lock does not qualify as a technological protection measure (TPM), then there will be no need to resort to the exemption. If it does, then the litigant has that recourse.

Finally, the Copyright Office should not deny this exemption out of concern that TracFone or other wireless carriers will suffer financial harm. If resellers are improperly depriving TracFone of income to which it has a valid legal right, TracFone has legal recourse beyond section 1201(a). It can continue to pursue its trademark infringement, unfair competition, tortious interference with business relationship and prospective advantage, false advertising, and harm to good will claims. Breach of

contract, unjust enrichment or civil conspiracy claims might also be brought. Courts, after full discovery from both parties, and with consideration of the law and policy behind these tort claims, are in the best position to make the proper determination about whether a particular actor improperly harmed the wireless carrier. Section 1201(a), however, makes no distinction between a recycling business, a business traveler and a trademark infringer or unfair competitor.

Neither carriers, handset manufacturers nor firmware purveyors has stepped forward to oppose this application. Moreover, granting an exception to a handset unlocker does not open the door to any infringing uses. Here, every unlocker is making a non-infringing use. Further, unlocking does not necessarily exacerbate the changes for others to infringe. Content on a handset platform can simply be locked in a way different from the way carriers lock handsets. There is no collateral damage to copyright interests from granting this exemption.

If at some point U.S. telecommunications policy in favor of greater competition in the wireless market is to change, Congress or the FCC should change it. Competition and consumer rights should not be impinged in favor of wireless carriers through a novel and unintended application of a copyright law. For these reasons, this request should be granted.

Burden of Proof

The subtext of the post-testimony questions is that the commentators have the burden to prove that section 1201(a) prohibits cell phone unlocking in every configuration and model. The questions also suggest that if the Copyright Office thinks unlocking is not covered by 1201(a), it will not grant an exemption. This is improper. Commentators need only show that the prohibition has or is likely to have a substantial adverse effect on non-infringing uses of a particular class of works.

To have a different burden of proof puts commentators in an untenable Catch-22. The applicability of section 1201(a) to unlocking is contingent on both the law and the model of phones at issue. Indeed, if sued, my

clients and other phone unlockers will argue that their activities are not violations of section 1201(a). To force us to characterize all unlocking as definitively illegal to gain an exemption would undermine our legal position should the exemption be denied and litigation commence. This office could deny the exemption for a myriad of reasons, including a finding that 1201(a) does not apply to unlocking at all. Yet, because we believe that an exemption from the Copyright Office is necessary to protect unlocking, we would be both forced to argue against our interests and forced to go on record contrary to what the Copyright Office's ultimate finding regarding legality might be.

That is why the actual burden of proof only requires us to show an adverse affect. We amply have met our burden of proof.

Overwhelming New Evidence of Actual Harm

Section 1201 has allowed wireless carriers to sue and extract settlements out of defendants. First, we pointed to the case of Soj Wireless. One of the claims was a violation of section 1201(a). The case settled with a permanent injunction prohibiting the defendants from altering or unlocking any TracFone phones. (Soj Wireless, Final Judgment and Permanent Injunction, Para. 3.ii., attached as Exhibit E).

Since that time, additional lawsuits claiming 1201 violations for cell phone unlocking have been filed.

On December 27, 2005, TracFone Wireless sued Pan Ocean Communications. The complaint alleged a violation of section 1201(a). The defendants settled the case on August 7, 2006 by entering into a permanent injunction. The injunction prohibits the defendants from "engaging in the alteration or unlocking of any TracFone phones". (Exhibit A, p. 3, para. 4.ii.)

On August 24, 2006, TracFone Wireless sued Larry's Cell. Count One of that complaint alleges defendants violated section 1201(a) by "individually act[ing] to and/or knowingly engag[ing] in a conspiracy to, avoid, bypass, remove, disable deactivate, or impair a technological

measure for effectively controlling access to the proprietary software within the TracFone Prepaid Software without TracFone's authority". (Exhibit B at p. 11, paras. 48, 43-50.)

On Tuesday, September 5, 2006, TracFone sent a vast number of threatening emails to businesses involved in the purchase of cell phones for unlocking and resale. (Exhibit C.) Several of these businesses have called counsel for commentators, who has referred them for legal advice. In the meanwhile, the threat of litigation actually interferes with legitimate unlocking businesses.

Even more worrisome for commentators, the Department of Justice filed charges in the Eastern District of Michigan against three Dallas men found in possession of approximately 1000 handsets. These men were in the business of traveling around the country buying phones at a low price and selling them for a higher price. The United States Attorney's Office charged the men with conspiracy to unlock cell phones and with money laundering. (United States v. Othman et. al. United States District Court, Eastern District of Michigan, Northern Division, Case No. 06-MJ-30401 BC, hereinafter Othman, attached as Exhibit F.) After a preliminary hearing on September 5, the Judge dismissed all the charges for lack of evidence. (Othman Docket Report, attached as Exhibit G.)

As in Sol Wireless, Pan Ocean, Larry's Cell, or Othman, commentators fear that a carrier may use 1201(a) to challenge their legitimate unlocking activity. The Wireless Alliance, for example, is in the business of unlocking phones for resale and recycle, just like these named defendants. If there is something wrong with what those defendants are doing, courts can adjudicate that behavior as unfair competition, trademark infringement, or some other business tort. Commentators have shown that U.S. policy as set forth by the Federal Communications Commission (FCC) favors unlocking. (Comments section III.B.2 (hereinafter COM) Section B.1.) If the FCC changes policy, it can issue new regulations that promote competition while protecting legitimate carrier business models. The Copyright Office, however, should not persist in allowing the misuse of section 1201(a) to chill non-infringing activity.

Questions Posed by the Copyright Office

Below, we have provided answers to the Copyright Office's additional questions. As the letter suggests, the answer to the questions varies depending upon the carrier, handset manufacturer, handset model, and firmware producer. (Testimony on pp. 14, ln 8-18 (hereinafter TEST)). Because phones have different chips, different operating systems and different configurations, it is very difficult to generalize as to what is true about mobile phone architecture.

More detailed information than that provided may be entirely under the exclusive control of the phone makers and network providers. Those parties did not contest this exemption and have not come forward with any information to counter the factual case for an exemption we have presented and documented. Commentators have made a strong and un rebutted case for an exemption. The unavailability of more detailed information is neither necessary nor a reason for denying our application. Answers, based on available information, are below.

- I. Explain how each of the types of software locks controls access to a copyrighted work.*

In general, software locks control access to copyrighted works by preventing the mobile phone user from operating or accessing the mobile firmware in conjunction with the network of the user's choosing. (TEST p. 9) We have identified and described four primary types of software locks that carriers currently use. The locking mechanisms include SPC locking, SOC locking, band order locking and SIM locking. (See, e.g., COM section III.B.2; TEST pp. 35-37.) SPC locking is the most common kind of lock for CDMA phones. SIM locking is most common for GSM phones.

SPC locking creates an access code that the user must input to instruct the phone to connect to a different network. The lock prevents the user from accessing and instructing the firmware that directs the phone to connect to a particular network.

SOC locking works the same way, but the SOC code is based on the carrier while the SPC code is based on the handset's ESN number.

Band order locking prevents a user from operating the mobile firmware on different frequencies.

SIM locking prevents an SIM card from communicating with the mobile firmware. The user cannot operate the firmware unless he uses the approved carrier's SIM card.

Each lock, whatever type, limits the customer's access to the handset firmware by stopping the user from operating the firmware on any network other than that approved by the carrier. Either these measures prevent the owner from reprogramming the firmware in his handset, in effect instructing it to run on a different network, or they stop the owner from operating the firmware inside the phone when he inserts a different SIM card.

II. Identify and describe the copyrighted work or works with respect to which access is controlled by the software lock.

The copyrighted work(s) to which access is controlled are "computer programs that operate wireless telecommunications handsets (Mobile firmware)". (COM section II, Reply section II (hereinafter REP).) In general, this firmware consists at minimum of a bootloader and an operating system. (TEST p. 9, ln 11-15). A bootloader is a special small program, the only function is to load other software for the operating system to start (http://en.wikipedia.org/wiki/Bootloader#Boot_loader). An operating system is a software program that manages the hardware and software resources of a computer. (http://en.wikipedia.org/wiki/Operating_system. A user needs to access a bootloader and operating system to operate any computer, including a mobile handset.

However, the essential software that operates a handset varies from model to model can be reconfigured and reprogrammed by carriers, manufacturers or software providers. This is why commentators are

asking for an exemption to circumvent TPMs that control access to whatever mobile firmware is required to operate their handset on the network of their choosing. (See TEST p. 75-76, specifying that the exemption is for the programs that allow the handset to connect to the network, including a bootloader, operating system and other programs that make the device into a phone.)

A. Who is the owner of that copyrighted work?

There is no way for commentators to know the answer to this question, any more than we could name the owner of the programs that make personal computers run. However, in TEST p. 63-64, commentators identify several handset operating systems, including ones presumably owned by Microsoft, Nokia, or offered as open source. Manufacturers may code and own their own firmware. They may license the firmware from some other company or individual.

Asking commentators to detail an answer to this question is deeply unfair, as even litigants in 1201(a) unlocking cases are not sure who owns the copyrighted work. For example, in Larry's Cell, TracFone claims that it owns the copyrighted work, "TracFone Prepaid Software". (Exhibit B, p. 3 para. 12.) However, in the dismissed criminal case of U.S. v. Othman, the government alleges that "Nokia installs proprietary software in the telephones which allows the telephones to be activated only by uses of a TracFone card." (Exhibit F, p. 3, para. 5.) If the United States government criminally charges people without knowing for sure who is the owner of the copyrighted work in a specific instance, commentators certainly cannot be expected to provide this information for all handsets that have ever been on the market and will be on the market for the next three years.

B. If the software lock controls access to only a portion of the work(s), identify both the works(s) and the portions(s) of the work(s).

Locking controls access to computer programs that operate wireless telecommunications handsets (mobile firmware). There are different

types of locks, and locking mechanisms are evolving. There are different handset software configurations, and these are changing. Commentators are asking for an exemption that allows circumvention of any software lock that controls access to any part of mobile firmware required to operate the handset on the network of the user's choice. Software is infinitely malleable. Any attempt by the Copyright Office to parse a highly technical exemption based on current specifications will just invite the carriers to program around the exemption. There is no reason to do this.

III. What information process or treatment must be applied in order to gain access to that copyrighted work(s)?

To gain access to the copyrighted work, you must break or circumvent the lock. There are many implementations of locks, and thus, many ways to circumvent them. One of the most common ways is by calculating the unlocking code that allows the user to instruct the phone to operate on a different network. Other methods may include flashing the chip (which does not always unlock the phone), or installing software that defeats the lock. This web link details one user's successful efforts to unlock his phone so that he could use his tri-band phone in Europe without paying long distance or roaming charges.

(http://www.oreillynet.com/onlamp/blog/2003/11/unlocking_your_nokia_phone.html). Clearly, this is just one example of how one person unlocked a particular phone. There may be many other ways.

IV. In what respect is access to that copyrighted work controlled by the software lock, including (but not limited to)

A. What is the nature of the access to the copyrighted work that is controlled by the software lock?

The user accesses the firmware to run the phone. The lock prevents the user from using (accessing) her phone's firmware. The nature of the access is purely functional. The lock controls functionality.

V. *How does the software lock control such access to the copyrighted work?*

See answer to I.

VI. *Describe whether and how the authority of the copyright owner of the copyrighted work is implicated in the operation of the software lock.*

Regardless of the type of lock or operating software used, the copyright owner has either affirmatively or implicitly agreed to the lock. The copyright owner generally affirmatively authorizes and works with the carrier to lock the phone. For example, with SPC locking, the most common lock for CDMA phones (e.g. Verizon), the carriers provide the algorithm to the manufacturers who input the ESN and use the resulting number to set an access code on new handsets. SOC locking works in a similar way, but the code is calculated differently. Every large carrier locks, and almost every phone manufacturer and firmware owner must do business with large carriers. Everyone in the manufacturing chain, hardware and software, either actively or implicitly permits the carriers to implement a lock that controls access to the firmware.

A. *Who installs and/or activates the software locks on the cellular phone handsets?*

Commentators cannot answer this question any more than we could identify who installs and configures software on personal computers. Most commonly, the manufacturer creates a fully functional phone consisting of both hardware and software. When a carrier orders a phone model, the carrier and the manufacturer work together to lock the phone. The firmware that is locked could be open source, owned by the carrier, owned by the manufacturer, owned by an operating system provider like Microsoft, or some combination of the above.

B. *Whether the software locks are applied "with the authority of the copyright owner".*

The locks are applied with the authority of the copyright owner, either because the owner explicitly agrees to, enables, licenses and/or participates in the locking, or at the very least because the copyright owner knows to an absolute certainty that its customers will lock the software and takes no steps to disallow it. The copyright owner has no choice. Carriers would refuse to buy any phone the manufacturer or firmware provider that does not allow them to lock.

C. If the locks are not installed by the copyright owner

i. What is the relationship between the owner and the installer?

The locks are installed with the authority of the copyright owner, if not physically by the copyright owner. The exact relationship, however, varies.

ii. Are the locks applied with the permission of the owner?

Yes, either explicitly or implicitly.

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

Owners authorize the imposition of TPMs through license, participation, agreement, enabling technology and/or actual knowledge and continued sales to the carriers.

VII. In what circumstances, if any, is access to the copyrighted work authorized by the copyright owner?

There is generally no relationship between the handset customers and the firmware owner where the firmware owner authorizes the handset user to access the copyrighted work. The user has the legal right to operate her handset (for which accessing the copyrighted work is required) as a result

of having bought the phone, not derived from any relationship or authorization by the owner.

Are software locks technological measures that “effectively control access to a work”?

Commentators believe that there is a colorable claim that software locks are TPMs, and for this reason, an exemption is warranted. We need not prove that all software locks are TPMs so long as section 1201(a) is being used to interfere with legitimate non-infringing activity, which it is.

CONCLUSION

Phone locking is contrary to American telecommunications policy, contributes to pollution and the digital divide and harms consumers. Section 1201(a) has actually interfered with the practice of phone unlocking, and will continue to do so. As a result, the legitimate non-infringing activities of Robert Pinkerton, The Wireless Alliance and other customers, phone resellers, and recyclers are chilled. It does not matter what lock is employed, what operating system is installed, or what programs are required to use a handset on a different network. The Copyright Office should issue an exemption for “computer programs that enable wireless telecommunications handsets to connect to a wireless communication network”. (TEST p. 48). This exemption has no demonstrated or theoretical effect on copyright infringement and, the balance of harms is greatly in our favor. We look forward to your decision.

EXHIBIT F



United States Copyright Office
Library of Congress • 101 Independence Avenue SE • Washington, DC 20559-6000 • www.copyright.gov

September 18, 2006

Morton David Goldberg, Esq.
Cowan, Liebowitz & Latman, P.C.
1133 Avenue of the Americas
New York, NY 10036-6799

Re: Copyright Office Docket No. RM 2005-11

Dear Mr. Goldberg:

The Copyright Office has received your letter of September 11, 2006 enclosing "Information Submitted on Behalf of CTIA – The Wireless Association, Complementing Response to Copyright Office Request of August 14, 2006 for Further Information."

As we assume you know, the deadline for initial comments in the above-referenced rulemaking proceeding was December 1, 2005. At that time, the Wireless Alliance submitted its comment requesting an exemption covering "computer programs that operate wireless telecommunications handsets. (Mobile firmware)." Comments expressing opposition to (or support for) that proposed exemption were due no later than February 2, 2006.

Persons wishing to express opposition to proposals for exemptions also had the opportunity to participate in hearings that took place last Spring. The hearing relating to the proposed exemption that is the subject of your submission took place on March 23, 2006. Following the hearings, if we determine that we require additional information or clarification on matters addressed by the witnesses who participated in the hearings, it has been our practice to submit additional questions to those witnesses seeking that information or clarification. However, those questions are not invitations for public comment. Once the hearings have concluded, the rulemaking proceeding is at an advanced stage and, apart from the information we elicit from the witnesses following the hearings, our rulemaking record is closed.

Our procedures do anticipate the possibility that someone may be able to justify submitting a comment to the Office after the deadlines for comments have passed. The final paragraph of our October 3, 2005 Federal Register notice initiating this proceeding stated:

To provide sufficient flexibility in this proceeding, in the event that unforeseen developments occur that would significantly affect the Register's recommendation, an opportunity to petition the Register for consideration of new information will be made available after the deadlines specified. A petition, including proposed new classes of works to be exempted, must be in writing and must set forth the reasons why the information could not have been made available earlier and why it should be considered by the Register after the deadline. A petition must also be accompanied by fifteen copies of any new proposed exemption that includes the proposed class of works to be exempted, a summary of the argument, the factual basis for such an exemption and the legal argument supporting such an exemption. These materials must be delivered to the Copyright Office at the address listed above. The Register will make a determination whether to accept such a petition based on the stage of the rulemaking process at which the request is made and the merits of the petition. If a petition is accepted, the Register will announce deadlines for comments in response to the petition.

Notice of Inquiry, Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, 70 Fed. Reg. 57526, 57531 (October 3, 2005).

Your September 11 letter and accompanying submission do not appear to have complied in form or substance, with the foregoing requirements.

If you wish to have us consider your September 11 letter and accompanying submission, we must receive, no later than 5:00 p.m. this Friday, September 22, the petition described in our Notice of Inquiry. Because you are not seeking an additional exemption, there obviously is no need to address "proposed new classes of works to be exempted." However, your petition must "set forth the reasons why the information could not have been made available earlier and why it should be considered by the Register after the deadline."

In addressing those reasons, we ask that you include the following information:

1. When did CTIA - The Wireless Association first become aware of:
 - A. The current rulemaking proceeding; and
 - B. The fact that the exemption upon which you now seek to comment was being sought?

2. Did any members of CTIA - The Wireless Association become aware of –
 - A. The current rulemaking proceeding; or
 - B. The fact that the exemption upon which you now seek to comment was being sought,
– prior to the time identified in response to question 1?

3. If the answer to question number 2 is “yes,” please:
 - A. Identify the member or members of CTIA - The Wireless Association in question;
 - B. State what information the member or members became aware of and when the member or members became aware of that information.

In addressing why your comments should be considered by the Register after the deadline, please explain the reasons for any delay from the time CTIA - The Wireless Association or any of its members first became aware of this rulemaking proceeding and the requested exemption, and address why those comments should be considered notwithstanding any such delay.

Sincerely,



David O. Carson
General Counsel

cc: Jennifer Granick, Esq.
Steven J. Metalitz, Esq.
Lance D. Reich, Esq.

EXHIBIT G



United States Copyright Office

Library of Congress • 101 Independence Avenue SE • Washington, DC 20559-6000 • www.copyright.gov

September 18, 2006

Jennifer Granick, Esq.
Stanford Law School Center for Internet & Society
Cyberlaw Clinic
559 Nathan Abbott Way
Stanford, CA 94305

Re: Copyright Office Docket No. RM 2005-11

Dear Ms. Granick:

The Copyright Office has received your letter of September 15, 2006 requesting an opportunity to reply to the submissions of CTIA – The Wireless Association and Tracfone Wireless.

Please understand that the Copyright Office did not solicit or encourage the submissions by these two organizations. You will have seen our letter of this date to Morton David Goldberg relating to the CTIA submission.

We understand your desire to have an opportunity to respond to these submissions. On the other hand, we remain hopeful that we will be able to conclude this rulemaking proceeding by October 28, when the exemptions for the following three years are to be announced. Because of the shortness of time, we do not believe we can accommodate your request to have until September 27 to submit a response. We will accept a response if it is received no later than the end of the day next Monday, September 25 (*i.e.*, if we have received an emailed copy by the time we arrive at our office the next morning).

Please note also that the Office has not yet made a determination whether to accept either of the submissions from CTIA or Tracfone. Because it is not likely that we will have made such a determination within the next week, and because there will be insufficient time following the time

Jennifer Granick, Esq.

-2-

September 18, 2006

such a determination is made to give you an opportunity to prepare a response at that time, you should assume for present purposes that we will be accepting the two submissions and provide us with any response you may have by the end of the day on September 25.

Sincerely,

A handwritten signature in black ink, appearing to read "David O. Carson", with a long horizontal flourish extending to the right.

David O. Carson
General Counsel

cc: Steven J. Metalitz
Morton David Goldberg
Lance D. Reich