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 section1201(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, tortuous 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 Sol 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. (Sol 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 unrebutted 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.