

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**

Testimony of Jennifer S. 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

On behalf of:

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

Introduction: Good morning. My name is Jennifer Granick, and I represent the Wireless Alliance and Robert Pinkerton. The Wireless Alliance recycles and resells used, refurbished, and new cellular products. The Alliance works with industry, refurbishers, and the Environmental Protection Agency to reduce toxic waste and help bridge the digital divide. In the Alliance's experience, phones that are not locked to a specific carrier are much easier to recycle and resell.

Robert Pinkerton is an individual residing in Arlington, Virginia who traveled frequently in his former capacity as Director of Government Solutions for Siebel Systems. Mr. Pinkerton, along with thousands of other Americans, has found that having a locked mobile phone has greatly interfered with his ability to communicate while traveling. We are asking the Copyright Office to grant an exemption under § 1201(a)(1) to allow individuals to unlock their cell phones so that they may use them with carriers of their choice.

Brief Summary of Argument: As the litigation in *TracFone v. Sol Wireless*¹ illustrates, Section 1201(a) is an actual threat to consumers seeking to unlock their cell phones. Cell phone unlocking is an otherwise legal and non-infringing activity and consumers should be able to unlock their phones without fear of liability. Unlocking to use the phone on the network of your choice is non-infringing. There is no option for most customers other than unlocking. Unlocking does not enable infringement of the firmware on the phone. Nor does unlocking necessarily hobble content companies in imposing digital rights management on audio-visual content stored on the phone. The balance of harms – particularly competition and consumer choice, environmental considerations, and the digital divide – greatly weighs in favor of this exemption.

This is a decision for the Copyright Office: In opposition to this application for an exemption, the content industry argues that a court or regulatory agency would first have to outlaw carrier's anticompetitive locking practices, and only

¹ *TracFone Wireless, Inc. v. Sol Wireless Group*, No. 05-232729, (S.D. Fla. Feb. 28, 2006). The Complaint is attached as Exhibit C, the Joint Stipulation for Entry of Final Judgment as Exhibit D, and the Final Judgment and Permanent Injunction as Exhibit E.

then would consumers have a right to self-help through unlocking. We need not prove that carrier locking is illegal to warrant an exemption for customer unlocking. Customer unlocking is legal, regardless of whether the carrier's practices are prohibited under antitrust law, agency regulations or state consumer protection statutes. The DMCA is the only reason consumers arguably can not engage in the otherwise legitimate activity of phone unlocking. Even if courts rule that carrier locking is unlawful, as they soon may², the DMCA would still outlaw unlocking and we would still be here seeking an exemption. So the response that this is in the wrong forum is ridiculous. Only the DMCA prevents unlocking and only the Copyright Office can grant an exemption to the DMCA.

Section 1201(A) Threatens Legitimate Unlocking: Nearly all wireless communications providers use software locks to tie a customer's handset to their service network. There are several methods of locking. In general, locking prevents the customer from accessing copyrighted mobile firmware (bootloader and operating system), and running that firmware in conjunction with the wireless network of their choosing.

The lock is a technological protection measure that controls access to a copyrighted work, i.e. the mobile firmware. Therefore, circumventing that lock arguably violates section 1201(a). Under the rule of *Lexmark Int'l, Inc. v. Static Control Components*, 387 F.3d 522 (6th Cir. 2004), a defendant in an anti-circumvention case could argue that unlocking is not illegal. In *Lexmark*, the Sixth

² There are pending state class action lawsuits against wireless carriers for locking practices. See, e.g., *In re CellPhone Termination Fee Cases*, J.C.C.P. 4332, Case No. RG04139536 (Alameda County Sup. Ct. filed June 24, 2005) attached as Exhibit F.

Circuit held that circumventing a secret handshake between a toner cartridge and a printer did not violate the DMCA because the handshake did not “effectively” control access to a copyrighted work. Rather, the purchase of the printer gave the owner access to the printer code. Similarly, purchasing a mobile phone may give the owner access to the firmware.

The Copyright Office should clarify that all mobile phone unlocking is legal under *Lexmark*, or in the alternative grant an exemption. Clarity from the Copyright Office, or an exemption, is required because, despite the rule of *Lexmark*, phone unlockers have been subject to suit and penalty under the DMCA.

Litigation between TracFone and Sol Wireless illustrates that section 1201(a) poses a real and actual threat to the non-infringing activity of cell phone unlocking. In *TracFone Wireless v. Sol Wireless Group, Inc.*,³ a small company in Florida was sued for purchasing prepaid wireless handsets, unlocking them, and then reselling them for use on other wireless carriers’ networks. Count Five of the complaint alleged that Sol Wireless violated section 1201(a)(1) by unlocking the handsets. On February 28, 2006, the trial court issued a permanent injunction against Sol Wireless that prevents it and its affiliates from “engaging in the alteration or unlocking of any TracFone phones”⁴. This outcome illustrates that even after *Lexmark*, section 1201(a) poses an actual harm to phone unlocking. This also disposes of the content industry’s objection that this

³ *TracFone Wireless, Inc. v. Sol Wireless Group*, No. 05-232729, (S.D. Fla. Feb. 28, 2006).

⁴ *Id.* at 4.

exemption is speculative.

All The Relevant Statutory Factors Support Granting The Exemption:

First, the vast majority of current and future mobile customers cannot unlock their phones without circumvention. Ninety-five percent of new subscribers have a choice of only four nationwide carriers, all of whom lock the handsets they sell.⁵

Second, allowing customers to change networks has no adverse affect on the market value of firmware. Customers buy firmware because it operates the handset, not as a commodity with independent value as a copyrighted work.

This is uncontested.

Finally, the balance of harms is in favor of unlocking. We have argued that unlocking helps customers far more than it hurts wireless carriers, and the public has resoundingly agreed. All the reply comments filed in response to this requested exemption, with the sole exception of the content industry's reply, support granting it. The thirteen comments tell personal stories of how locking deprives customers of the full value of their cell phones. For example, Michael Ditmore had to buy a new phone simply because two carriers consolidated. Jonathan Butler's phone and bluetooth accessories are now just "expensive paperweights". Everett Vinzant lost \$1200 because his carrier wouldn't unlock his

⁵ For example, a class action lawsuit filed initially in Los Angeles by the Foundation for Taxpayer and Consumer Rights against AT&T, T-Mobile and Cingular alleges that Cingular will not unlock customer phones unless their contract has expired. *See Foundation for Taxpayer and Consumer Rights v. AT&T*, Case No. BC 316619 (Los Angeles County Sup. Ct. June 7, 2004), attached as Exhibit G. The case was coordinated with pending cases in Alameda County and is now part of the *In re Cellphone Termination Fee Cases*. In the amended complaint filed in that matter, the class alleges that even after a contract has expired, wireless carriers refuse to unlock previous subscribers' handsets. *See Complaint at 3, In re CellPhone Termination Fee Cases* (Alameda County Sup. Ct. June 24, 2005) (No. J.C.C.P. 4332).

phone.

Unlocking allows customers to use the wireless products they have already purchased, and helps customers to choose among competing service providers. This is precisely the kind of competition that is consonant with U.S. telecommunications policy. Wireless providers may claim they need software locks because they subsidize the price of the handset and they want to make up the difference by ensuring that the customer uses the carrier's service. However, legally enforceable service contracts provide for a minimum monthly fee and a hefty early termination penalty. These contracts ensure that carriers receive every legitimate benefit of the subsidy they provide.

The environment benefits from unlocking because more handsets can be sold on a secondary market. That means less toxic chemicals end up in landfills, incinerators and ground water. As our written comments show, the proliferation of second-hand handsets will help address the digital divide problem, particularly in developing nations.

Most importantly, there is no evidence that phone unlocking threatens the rights of the content industry. Increasingly customers use handsets for accessing, storing, using (not to mention creating) copyrighted materials. The exemption we are requesting is *narrowly drawn*: We are asking for an exemption that would *only* allow an individual to circumvent a TPM (technological protection measure) that controls access to the software that connects the phone to a carrier's network. This exemption does not allow circumvention of TPMs that

control access to audiovisual material on a handset.

Granting an exemption for circumventing a process that allows a consumer to access the mobile phone firmware (boot process and operating system) does not necessarily open the door to circumvention of a process that controls access to or copying of audio-visual works. The content industry's reply comments finesse this by say that a mobile devices' functions of accessing, receiving, playing back, storing and copying copyright materials **may be** controlled by the same programs that connect the user to the dial tone provided by a particular network. The content industry knows how it protects its works, but it provides no evidence that that protection is or must be controlled by the same firmware that operates the phone on the network of the customer's choosing.

Modern cell phones are built like ordinary personal computers. Cell phones generally have a processor, a bootloader that starts the operating system, an operating system, a set of applications, and data files. The way these layers interact in mobile phones differs, not just from carrier to carrier, but from model to model. Because phones have different chips, different operating systems, and different configurations, it is difficult to generalize.

Publicly available documents about mobile phone technology show that DRM and content playback happens at a different layer than locking. For example, the Open Mobile Alliance is a consortium of technology companies, including content providers, promoting an open digital rights management standard.⁷ The OMA standard is used by a significant percentage of the mobile device market. The

⁷ <http://www.openmobilealliance.org/>, attached as Exhibit H.

OMA architecture places DRM functionality at a different layer than Service Provider functionality.⁸ This proves that DRM is not necessarily entwined with “accessing a dial tone”. These are different functionalities.

Different mobile devices will deal with DRM and service provision functions differently. Even if some carriers may currently place DRM technology at the firmware layer, the OMA standard does not require this architecture for DRM to work. The content industry, in collaboration with the carriers and manufacturers, can simply choose to store the keys elsewhere, as is currently the case with many handsets on the market.

CONCLUSION: This application for an exemption should be granted. Members of the public have written to the Copyright Office asking that the right to unlock their phones be returned to them. Unlocking promotes competition, environmentalism and social equality. At the same time, there is no evidence that unlocking encourages or enables infringement. The Copyright Office should remove the only legal barrier to this non-infringing, socially beneficial conduct, by either indicating that unlocking is not illegal under *Lexmark* or by granting the exemption.

⁸ http://www.lockstream.com/products_OMA_2.html, attached as Exhibit I.

EXHIBIT A

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**

Comments of

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

I. THE COMMENTING PARTIES

The Wireless Alliance is a Colorado limited liability corporation that recycles and resells used, refurbished, and new cellular products. Each mobile unit contains toxic materials including lead, cadmium and beryllium. Mobile phones that are thrown away end up in landfills and these metals then leach into the water table. The Wireless Alliance helps the environment by repurposing used phones and recycling those that cannot be reused. The Wireless Alliance sells between 20-60,000 phones per month, including CDMA, TDMA, Analog, and GSM. By working with industry, refurbishers, the Environmental Protection Agency and charities, The Wireless Alliance both reduces toxic waste and helps bridge the digital divide between the United States and third world countries.

Robert Pinkerton is an individual residing in Arlington, Virginia. Pinkerton was the

Director of Government Solutions for Siebel Systems, Inc. until November 2005 and now works for Lexis Nexis. As Siebel's Director of Products Group for the Public Sector in 2002 and 2003, Pinkerton traveled over 100,000 miles per year for work. The position required him to travel regularly from the East Coast to California, Europe and Africa. During those trips, Pinkerton wanted to use his mobile phone to keep in contact with his company and his family, but the phone did not work in most of the locations Pinkerton visited. Renting a phone at the destination airport is expensive, time consuming, and requires Pinkerton to carry both his PDA and rental. Moreover, because recipients do not recognize the rental calling number, they rarely will answer his incoming calls. Because Pinkerton cannot unlock his phone and use it on European networks, he often travels without mobile phone service.

II. INTRODUCTION

The commenters submit the following comments in connection with the Copyright Office's October 3, 2005 Notice of Inquiry.¹ The commenting parties propose exemptions from the Section 1201(a)(1)² prohibition on the circumvention of technological measures that control access to copyrighted works for the following class of works:

Computer programs that operate wireless telecommunications handsets. (Mobile firmware)

In October of 2005, a major mobile handset manufacturer sent a legal threat to a business that distributes phone unlocking software, claiming Digital Millennium Copyright Act violations. Phone unlocking software is a tool that can circumvent the software locks carriers use to stop customers from using the handsets they purchase on competing mobile networks. Though the threat did not identify a specific statute, counsel for commenters Pinkerton and The Wireless Alliance also advised the unlocking business, and believes that the manufacturer is claiming that provision of unlocking software, because it circumvents the software locks that control access to the mobile firmware, violates section 1201(b).³ The cease and desist letter shows that handset manufacturers and carriers are imminently planning to use section 1201 to stop phone unlocking.

Using a mobile handset on a different network is clearly non-infringing activity. The customer is not copying the firmware, nor is he exercising any exclusive right the copyright owner has in the mobile firmware. Rather, the circumventor accesses the firmware merely to reprogram it to work on a different network, or to utilize a different SIM card. The customer merely wants the handset to run on the network of his choice.

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

² Unless otherwise noted, all section references are to the current Title 17 of the U.S. Code.

³ See, Jennifer S. Granick, "Free the Cell Phone", Wired News, September 28, 2005, available at <http://www.wired.com/news/culture/0,1284,68989,00.html>

III. PROPOSED EXEMPTION

A. Summary

Mobile communications providers are using software locks to control customer access to mobile phone operating software embedded inside the devices. These locks prevent customers from using their handsets on a competitor's network. Customers who want to use their handsets on a different network must circumvent the locking software to access the computer program that allows the phone to operate (mobile firmware). Mobile providers can use section 1201(a) to stop customers from selecting a provider of their choice, resulting in poorer service and higher costs for customers, reduced competition contrary to explicit U.S. policy, and environmental disaster as a result of mobile handset waste. Locked phones also contribute to the problem of the digital divide between rich and poorer nations.

B. Facts

1. Scope of the Problem

a. Bundling Handsets with Service is a Common Practice, But is Contrary to Explicit U.S. Telecommunications Policy

In the United States, wireless communications carriers like Verizon or Sprint (carriers) use spectrum licensed to them by the Federal Communications Commission (FCC) to provide mobile phone service to customers. Mobile service uses different technological standards, and there are presently three main mobile networks in the United States, GSM, CDMA and TDMA. Customers access these networks with mobile phones, or handsets, compatible with one or more of these standards. CDMA phones do not necessarily work on GSM networks. However, a CDMA phone is capable of operating on any CDMA network.

In 1992, the FCC expressed its concern that carriers were bundling handset sales with service contracts. Specifically, the carriers were requiring customers to purchase their handsets directly from the carriers or authorize agents and to contract to pay for a minimum amount of wireless airtime per month over a period of a year or more. Based on these practices, the FCC stated its "concern that customers have the ability to choose their own CPE [handset] and service packages to meet their own communications needs and that they not be forced to buy unwanted carrier-provided CPE [handsets] in order to obtain necessary services." In the Matter of Bundling of Cellular Customer Premises Equipment and Cellular Service, CC Docket No. 91-34, 1992 WL 689944 (F.C.C. June 10, 1992), at para. 6 (hereinafter "1992 FCC Bundling Ruling"). But, because in 1992 there were low barriers to entry in the handset market, a wide selection of handsets from which customers could choose, no evidence that carriers were refusing service to customers that purchased other brands of handsets, and a geographically fragmented market, the FCC permitted carriers to continue to offer handsets and services as a

bundled package so long as service was not conditioned on purchasing the handset from the carrier. 1992 FCC Bundling Ruling, paras. 8, 15.

Despite this ruling almost every carrier today forces customers to purchase handsets directly from the carrier or its approved agents in order to get mobile service. Additionally, once the customer enters into a service agreement, the carriers use a variety of techniques to prevent customers from switching to competitor carriers, whether before or after the term of the service contract has passed.

Until recently, one effective anti-competitive practice was that carriers refused to allow customers to transfer their mobile phone numbers when they switched providers. Customers who wanted to keep their familiar phone numbers were stuck with their carrier, regardless of service quality, price, or terms of provision. With the Telecommunications Act of 1996, however, Congress mandated that carriers offer number portability in accordance with regulations to be promulgated by the FCC. 47 U.S.C. 251(b)(2). The purpose of this obligation, and others in the 1996 Act, is to “promote competition and reduce regulation . . . to secure lower prices and higher quality services for American telecommunications consumers and encourage the rapid deployment of new telecommunications technologies.” Telecommunications Act of 1996, HR 155, S 652, Beginning, *available at* <http://thomas.loc.gov/cgi-bin/query/F?c104:4:./temp/~c104W0zTCP:e0:>

Today, carriers’ anti-competitive practices continue to include the tying policy that forces customers to purchase handsets from the carrier or a designated agent, limits on the availability of handsets from other sources, restrictions on the ways in which dealers are permitted to market handsets, and locking the handset to prevent use with a competitor carrier.

Nearly all wireless communications providers use software locks to tie a customer’s handset to their service network. There are several types of locking software that work in different ways. In general, the software prevents the customer from accessing copyrighted mobile firmware, an act necessary to either instruct the phone to connect to a different carrier or to program the handset with the secret handshake a competing carrier provides to customers connecting with its network.

Customers who unlock their phones to use them on a different network are not infringing any copyright-protected interest of the carriers. Yet, if the Copyright Office does not grant an exemption, carriers may levy anti-circumvention claims against customers who unlock their phones and give legal force to a business practice that Congress and the FCC have explicitly stated they do not support.

b. Locking Hurts Competition and Innovation

Locked phones limit competition in the mobile communications market, contrary to explicit U.S. policy. As a result, customers get poorer service, higher prices and reduced innovation. Companies have reduced incentives to improve their networks, because

customers are less likely to change to a competitor.

The problem is much worse today than it was in 1992. Today, there are fewer carriers, no more spectrum to allocate to newcomers, and fewer equipment manufacturers. There is also now a well-established practice of forcing customers to buy unwanted handsets in order to get service. Even worse, as equipment becomes more expensive customers are increasingly stuck. Today, many mobile customers spend hundreds of dollars on a handset only to find they have to throw that handset away and purchase a new one if they want to change carriers. This discourages customers from selecting the carrier of their choice.

Locking artificially prevents a customer from using their phone on another network when changing carriers, even when that phone would otherwise be fully functional on that network. When commentator Pinkerton signed up for service from Sprint in 2000, he found that his phone was useless when he traveled outside of the U.S. Because the handset was locked, Pinkerton could not switch to a European carrier for the duration of his visit. As a result, he traveled without mobile phone service. At the end of 2002 and 2003, Pinkerton switched to a GSM phone from T-Mobile. He found there that the reverse was true. The service was great in Europe, but terrible in the U.S. Unable to unlock his phone, and locked into a one-year contract through his company, Pinkerton suffered unreliable service whenever he was in the country and when he traveled outside of Europe. During one business trip to South Africa, Pinkerton's wife desperately tried to reach him to confer on the details of a bid the family would place on a home in the competitive Arlington housing market. She was unsuccessful, and the Pinkertons did not get the house. Despite the poor service, and the fact that he never was able to clearly connect with his wife, the trip to South Africa resulted in the largest bill Pinkerton has ever received.

c. Locking Hurts the Environment

When Americans find that they can't unlock their phones and use them with a new service provider, they throw their old phones away. Americans discard over 150 million mobile phones a year. These phones are filled with toxic chemicals like lead, copper, antimony, beryllium, cadmium, and zinc. These chemicals are released into the air when the phones are incinerated and leached into the groundwater when the phones are cast into landfill, threatening human health and the environment. By some estimates, discarded phones, phone batteries and their accessories produce 65,000 tons of toxic trash a year.

Handset resellers help the environment by keeping perfectly functional handsets out of landfills and in the hands of customers. Commenter The Wireless Alliance (TWA) collects handsets and distributes them to resellers or recycles them in accordance with Environmental Protection Agency policy. TWA is able to repurpose almost 65% of handsets it collects.

Resellers and refurbishers find that handsets are more marketable when customers can

use them on any network, not just the one to which it was originally tied. TWA estimates that if participants in the used handset market were allowed to unlock handsets, it could recycle several hundred thousand more phones a year, keeping that much more toxic metals out of our air and water.

d. Locking contributes to the Digital Divide

Unlocking also makes used phones more flexible, marketable and useful to second-hand customers around the world. When phones are locked to U.S. carriers' networks, they often do not work in other countries. This exacerbates the "digital divide" between rich and poor nations. In March of this year, the United Nations launched a Digital Solidarity Fund to address "the uneven distribution and use of new information and communication technologies" between nations. Recently, The Economist noted that the best way to begin to address the digital divide was to promote the spread of mobile phones, rather than of personal computers. "The Real Digital Divide", The Economist, March 10, 2005.

As the article states:

Plenty of evidence suggests that the mobile phone is the technology with the greatest impact on development. A new paper finds that mobile phones raise long-term growth rates, that their impact is twice as big in developing nations as in developed ones, and that an extra ten phones per 100 people in a typical developing country increases GDP growth by 0.6 percentage points.

Moreover, "Mobile phones do not rely on a permanent electricity supply and can be used by people who cannot read or write." According to the World Bank, 77% of the world's population lives within range of mobile communications service networks. If these people had inexpensive used handsets that would work on those networks, it would have a strong positive effect on GDP and improve not only the digital divide problem, but also the underlying problem of poverty itself. Locked handsets that end up in landfill could be in the hands of Africans, bridging the digital divide and reducing poverty.

e. Mobile Locking Has Severe Adverse Consequences

The scope of the problem of phone locking is vast and severe. Locking mobile phones harms American customers in ways that are directly contrary to U.S. telecommunications policy. It harms the environment by encouraging customers to throw away perfectly good phones that could be repurposed and sold on the used market. Locking also perpetuates world poverty by reducing the number of usable, affordable handsets that can be exported to impoverished nations around the world.

2. Technological Protection Measures Involved

Handset locking software varies depending on the type of network and the handset equipment.

a. SPC locking

Sprint and Verizon both employ SPC (service provider code) locks on their handsets. The SPC code is a number derived from an algorithm that uses the handset's ESN (electronic serial number). 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. An SPC locked handset cannot be reprogrammed to operate on a mobile network unless the programmer first inputs the correct SPC code. By blocking access to programming with an SPC lock, the carrier can ensure that its handsets cannot be reprogrammed for use with other carriers.

b. SOC locking

AT&T Wireless and Cingular use SOC (system operator code) locks. The SOC is a number assigned to a carrier. The code programmed into the handset must match the code of the carrier providing service to the phone. When the handsets are locked, the SOC code cannot be changed, so the handset cannot be reprogrammed for use on a different network.

c. Band Order Locking

Some carriers also use band order locking, which restricts the frequencies on which handsets will operate. While handsets are generally capable of operating across the entire range of frequencies allocated by the FCC for mobile communications, each carrier is licensed to operate only on certain blocks within those bands. By restricting the blocks on which the handset can operate, the carrier prevents the handset from being used on a different network.

d. SIM locking

A SIM card is a small device that stores a customer's identifying information in some handsets, especially GSM handsets. The card is easily removed and replaced. A customer with a SIM card phone can easily select service providers by popping the appropriate card in the handset. The network reads the card, allows the connection and collects accurate billing information from the card. AT&T and other carriers program their handsets with SIM locks to prevent them from operating if a different SIM card is inserted into the handset.

All these technological measures control access to the copyrighted software inside the mobile handset. Either these measures prevent the owner from reprogramming the firmware in his handset, or they stop the owner from operating the firmware inside the phone when he inserts a different SIM card.

C. An Exemption from section 1201(a) for Circumvention of Any Locking

Mechanism that Controls Access to Software Inside a Mobile Handset is Both Appropriate and Necessary

Locking software is a technological protection measure that effectively controls access to the copyrighted mobile firmware. Mobile handset locking, whether it is SPC, SOC, Band Order or SIM, effectively controls access to the copyrighted software that operates mobile phones (mobile firmware). If the phone is locked with SPC, SOC or Band Order locking, the customer cannot program the mobile firmware to connect to the network of her choice. If the phone is locked with SIM locking, the customer cannot access the mobile firmware with a different SIM card. Unlocking, or circumventing SPC, SOC, Band Order, SIM and/or other locking techniques is required to run, or access, mobile firmware.

The prohibition on circumventing locking software inhibits customers from using their handsets on other networks. When handsets are locked, the customer must use the network of the carrier that sold him the handset and cannot switch to another provider without unlocking the handset and thereby accessing the mobile firmware. Since section 1201(a) prohibits circumvention to access the copyrighted software that operates a mobile handset, customers are unable to switch networks.

Using a mobile handset on a different network is clearly non-infringing activity. The customer is not copying the firmware, nor is he exercising any exclusive right the copyright owner has in the mobile firmware.

Even if reprogramming is viewed as making an adaptation of the copyrighted work, the adaptation is non-infringing under section 117. Section 117 authorizes the owner of a copy of a computer program to adapt it “as an essential step in the utilization of the computer program in conjunction with a machine” if it is used for no other purpose. Under 17 U.S.C. 117, a legitimate owner of a copy of a program has the “right of adaptation,” which includes “the right to add features to the program that were not present at the time of rightful acquisition.”⁴ In *Aymes v. Bonelli*⁵, the Second Circuit held that the rightful possessor of a copy of a software program can make modifications to that program to suit his own needs. In *Aymes*, the appellate court stated that “[b]uyers should be able to adapt a purchased program for use on the buyer’s computer because without modifications, the program may work improperly, if at all. No buyer would pay for a program without such a right.”⁶ “[The defendants], as rightful owners of a copy of the plaintiff’s program, did not infringe upon the copyright, because the changes made to the program were necessary measures in their continuing use of the software in operating their business and the program was not marketed, manufactured, distributed, transferred, or used for any purpose other than the defendant’s own internal business needs.”⁷ As with the defendants in *Pfortmiller* and *Aymes*, the mobile handset owner simply wants to

⁴ *Foresight Resources Corp. v. Pfortmiller* 719 F.Supp. 1006, 1009 (D. Kan. 1989).

⁵ (2nd Cir. 1995) 47 F.3d 23, 26

⁶ *Id.*

⁷ (*Id.* [citing 17 U.S.C. 117(1) (1992)].)

program his copy of firmware for the sole purpose of continuing to use it in operating the handset. This is a non-infringing use under section 117.

The holdings of *Chamberlain Group Inc. v. Skylink Technologies Inc.*⁸, *Lexmark v. Static Control Components*⁹ and *StorageTek v. Custom Hardware Engineering & Consulting*¹⁰ would not ensure that consumers who want to unlock their mobile phones will not be sued under section 1201. Given the disparity in resources between an individual customer and the multi-billion dollar carriers, even a low level of legal uncertainty will have a large chilling effect on unlocking activities that a court might later find legitimate. Only an explicit exemption will assure customers that phone unlocking will not be challenged in the courts

In *Chamberlain Group Inc. v. Skylink Technologies Inc.*, the defendant manufactured and sold a device that would open a variety of garage door openers, including those manufactured by the plaintiff. The plaintiff argued that the defendant mimicked its rolling code technology to make use of, or “access” the code that opened the garage door and that the defendant’s GDO was therefore an illegal circumvention device under the DMCA. The trial court rejected this claim on the grounds that the compatible transmitters opened garage doors only if homeowners inputted the transmitter signal into the GDO. The homeowner is authorized to access the plaintiff’s code with any GDO because the plaintiff did not place any contractual restrictions on the type of transmitters homeowners are permitted to use.¹¹

Today, some mobile phone carriers inform customers in the document setting forth the Terms of Service that they may not program their phones to run on competing networks.¹² Others may soon follow. Carriers may argue that a “Terms of Service” document that states that the customer does not have authorization to reprogram the handset for use on another network distinguishes their circumvention claim from that in *Chamberlain*.

In *Lexmark v. Static Control Components*, the Sixth Circuit reversed a trial court ruling that a printer cartridge compatible with the plaintiff’s printers was an illegal circumvention device. The appellate court held that the printer owners gained unfettered access to the copyrighted Printer Engine Program when they purchased the printer, and that the authentication sequence between the cartridge and the printer closed one avenue of access but left the others open, including leaving the code freely readable to any

⁸ 381 F.3d 1178 (Fed.Cir. 2004).

⁹ 387 F.3d 522 (6th Cir. 2004).

¹⁰ 421 F.3d 1307 (Fed.Cir. 2004).

¹¹ 381 F.3d at 1187.

¹² See http://www.t-mobile.com/info/legal/terms_cond.asp, T-Mobile Terms and Conditions, para. 8, “A T-Mobile Phone may be programmed to accept only a T-Mobile SIM card.”

printer owner. Therefore, the authentication sequence did not “effectively control access” to the copyrighted work.¹³

Owners of most mobile handsets are not able to freely read the computer program that runs the handset. The locking software categorically controls user access to the code that performs certain programming functions. Carriers may argue that the locking mechanism, unlike the “secret handshake” in *Lexmark*, is a measure that does effectively control access to the mobile configuration firmware.

In *StorageTek v. Custom Hardware Engineering & Consulting*, the plaintiff sued an independent company that repairs the databases plaintiff manufactures. To diagnose problems, the defendant had to circumvent a technological protection measure in order to access diagnostic information and error codes. The Federal Circuit first found that the defendant’s actions fell within the safe harbor of section 117, which allows copying for repair and maintenance. Next, the court rejected the plaintiff’s section 1201 claim, holding that, because the repair activity was non-infringing, there could be no DMCA violation. “To the extent that StorageTek’s rights under copyright law are not at risk, the DMCA does not create a new source of liability.”¹⁴

Accessing the mobile firmware to reprogram the handset for different networks is non-infringing activity. However, accessing other portions of the firmware may implicate copyrights, not of the carrier or manufacturer, but of their content partners that sell games, ringtones, photos and videos for mobile devices. Mobile firmware often includes digital rights management software (DRM) that prevents unauthorized copying or forwarding of this content. Carriers may argue that they refuse user access to the firmware in order to protect the DRM that protects these third party copyrights. Since there is some relationship, though attenuated, between access controls on the firmware and copyrights, *StorageTek* may not protect mobile phone unlockers. Of course, the requested exemption does not include circumvention of DRM to access the class of works that includes copyrighted games, ringtones or other creative content. The requested exemption only includes circumvention of locking codes to access the class of computer programs that operate mobile devices.

Congress has never considered the exemption the commenters propose. Congress did set forth in section 1201(f) a reverse engineering exception. That exception contemplates a circumventor who seeks to create an independent interoperable computer program. It does not imagine the situation that the commenters encounter, where they need to circumvent in order to use a physical device they already legitimately possess in a legal manner. The Librarian should therefore feel free to establish this exemption under its statutory authority.

Because section 1201 prohibits phone unlocking and because phone unlocking is a desirable, non-infringing activity, the Librarian should grant this exemption.

¹³ 387 F.3d at 546-47.

¹⁴ 421 F.3d at 1318.

D. Statutory Factors

Section 1201(a)(1)(C) directs the Copyright Office to consider the following when crafting exemptions:

- (i) the availability for use of copyrighted works;
- (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes;
- (iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research;
- (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and
- (v) such other factors as the Librarian considers appropriate.

All relevant factors mitigate in favor of the proposed exemption.

1. Accessing one's own mobile firmware is unavailable without circumvention.

The vast majority of current and future mobile customers cannot unlock their phones without circumvention. Customers have very few options for mobile service other than the major wireless carriers. According to a January 2005 Business Week analysis, 95% of new subscribers have a choice of only four nationwide carriers.¹⁵ These are Verizon, Cingular, Sprint and T-Mobile, all of whom lock the handsets they sell.

2. Availability for Use by Nonprofit Archival, Preservation and Educational Purposes.

The commenting parties do not believe that this factor is relevant to the instant exemption.

3. Impact on Criticism, Comment, News Reporting, Teaching, Scholarship, or Research

The commenting parties do not believe that this factor is relevant to the instant exemption.

4. Impact on Market for or Value of the Protected Work

¹⁵ http://www.businessweek.com/investor/content/jan2005/pi20050120_9922.htm

Allowing customers to change networks has little to no adverse affect on the market for handsets. Wireless providers may claim they need software locks because they subsidize the price of the handset and they want to make up the difference by ensuring that the customer uses the carrier's service. However, every new customer signs a legally enforceable contract that provides for a minimum monthly fee and a hefty early termination penalty. These contracts ensure that customers bear at least the cost of any subsidy in their monthly fees, if not more. As a result, a carrier receives every legitimate benefit of the subsidy it provides. It goes without saying that the customer's financial obligation under the service contract is unaffected by unlocking. Unlocking merely allows the customer to use the same handset with a different carrier, paying an additional amount to that carrier for the service during the period of the contract, or to take their handset to a new provider if desired at the end of the contract period. Permitting unlocking will not raise the consumer price of handsets. In fact, it may lower the price of handsets and of wireless service by making mobile phone markets more competitive.

5. Other Factors

The commenting parties urge the Copyright Office to consider the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on the environment and on international poverty. Allowing customers and handset resellers to unlock phones would mitigate the massive waste problem created when people throw away their handsets to switch carriers. It would also enable used phones to work on more networks, making them more versatile and saleable for second-hand purchasers. Finally, handsets can be exported to impoverished nations, increasing their GDP and reducing the digital divide.

F. Balance of Harms

In balance, consumers, the environment and the international community suffer far, far more from handset locking than mobile providers legitimately benefit. Increased competition in the mobile service market has been the official United States policy since 1992. To improve competition, it has been national policy to enable customers to more freely switch providers. This is why Congress mandated number portability in 1996. Since then, the wireless market has consolidated even further, so pro-competitive policies are even more important. The FCC does not yet prohibit handset locking, though in March of 2004 consumer groups began urging it to do so.¹⁶ Yet, section 1201(a) prohibits the legitimate owners of handsets from unlocking. This inequity strikes the opposite balance sought in the 1996 Telecommunications Act. It is anti-competitive and adversely consumer choice in handsets and providers, increasing prices and reducing incentives for service improvements and handset innovations.

Locking also has the unintended but dramatic consequence of poisoning our air and

¹⁶See Consumer's Union letter, *available at* <http://www.consumersunion.org/campaigns/handset%20locking%20letter%20FCC%20-%20mar%202011%202004.pdf>

water. If customers could continue to use their handsets at the end of the term of their service contract, we could prevent thousands of tons of toxic waste every year. These repurposed handsets would not only help customers in the United States, but they could contribute favorably to economic growth in developing nations. In fact, mobile phones may prove far more valuable to impoverished countries than computers because they are easy to use, need less maintenance, and readily cross the language barrier.

The Copyright Office should not allow mobile providers to use the anti-circumvention provisions in order to obtain legal protection for an anti-competitive business practice that the FCC and Congress have explicitly rejected. If this exemption were granted, carriers would still be allowed to lock their handsets, but motivated customers could unlock their handsets if it was worth the trouble to do so. These customers would continue to pay their monthly service fees under their service contracts, and would be subject to penalties if they terminated their contracts early. When in Europe, their business associates and families could continue to reach them on their personal handset. While it may economically benefit carriers, they have no legitimate interest in forcing customers to continue with an inferior provider simply because they invested in a handset or to purchase a new handset simply to get wireless service.

VII. Conclusion

For the reasons set forth above, the commenting parties respectfully request that the Copyright Office Register recommends to the Librarian that the proposed exemption herein be granted.

EXHIBIT B

