



1776 K STREET NW
WASHINGTON, DC 20006
PHONE 202.719.7000
FAX 202.719.7049

7925 JONES BRANCH DRIVE
McLEAN, VA 22102
PHONE 703.905.2800
FAX 703.905.2820

www.wileyrein.com

July 13, 2009

Bruce G. Joseph
202.719.7258
bjoseph@wileyrein.com

VIA ELECTRONIC MAIL

Rob Kasunic
Principal Legal Advisor
Office of the General Counsel
United States Copyright Office
101 Independence Avenue, SE
Washington, DC 20559
rkas@loc.gov

**Re: Response to Copyright Office's Questions Posed in the 2009 Section
1201 Anticircumvention Rulemaking**

Dear Mr. Kasunic:

CTIA – the Wireless Association® respectfully submits the following responses to the questions asked in your June 23, 2009 letter relating to cell phone unlocking.

- 1. Virgin Mobile USA testified that due to the inexpensive nature of the chip used on many of its subsidized handsets, there was no practical or cost-effective way to use separate technological measures to protect (1) the firmware and (2) the copyrighted works (such as ringtones, wallpaper or screensavers) contained on its handsets. Do any other manufacturers use the same or substantially similar chipsets but with separate protection measures on (2)? Are equally or nearly-equally inexpensive chipsets available that can accommodate such separate technological measures? In other words, in order to control cost, is it necessary to protect different copyrighted works contained on such handsets with one technological protection measure that controls access?**

CTIA Response: This question is not susceptible of a simple answer. Chipsets must be designed and then developed and optimized for specific uses on specific devices. Power consumption and computing demands vary from device to device. Evaluation of the capability of any given chipset on any given device involves a significant engineering exercise that CTIA and its members are not able to undertake. Further, CTIA is not aware of the identity of the chipsets used by Virgin Mobile, the performance demands imposed by Virgin Mobile's devices, or the level of performance specified by Virgin Mobile, as this information is confidential.

Rob Kasunic
July 13, 2009
Page 2

More fundamentally, the question appears to reflect a misunderstanding of important principles of digital security on mobile devices, as it appears to assume that where additional DRM-based security is applied to content, beyond the security that locks the phone, the added security is a “separate technological protection measure” from that applied to the phone’s operating system (*e.g.*, encryption that is separate from the operating system). CTIA’s understanding is to the contrary – even where added technological protection measures are used, they are often measures that are layered on top of the operating system and that are implemented and enforced by the operating system. This is true even on phones provided by carriers other than Virgin Mobile. In other words, with respect to significant copyrighted content on a wide variety of phones, technological protection is based on usage rules imposed by the content provider that are enforced by the phone’s operating system, or by applications that are, in turn, protected by the operating system. Moreover, these technological protection measures often do not involve encryption, so the content remains in the clear. A hack of the security protecting the operating system can open the door to this content. The phone lock protecting the operating system may be thought of as the keys on the door of a house. Once the door is unlocked, and the operating system is exposed, the contents of the house may be available for the taking.

While it is possible in some circumstances to use encryption-based technology to provide additional protection for certain content, the obligation to decrypt the content each time it is accessed imposes additional power and processing burdens on the device that can degrade the consumer experience (*e.g.*, by limiting battery life). As a result, encryption-based technology often is disfavored.

Further, even where content encryption is used, layering of security technology is an important strategy to protect content. In other words, the phone lock often provides added protection to encrypted content by limiting access to the operating system and, in turn, to the content or to encryption keys that may be present on the device. As a legal matter, there is nothing in section 1201 that obligates copyright owners or their partners to rely on a single layer of security, and there is nothing in section 1201 that permits circumvention of a first layer of security as long as a second layer is present. As a matter of good security practice, it would make no sense to limit copyright owners to the use of a single layer of security protected by the prohibitions of section 1201.

