

Before the  
UNITED STATES COPYRIGHT OFFICE  
LIBRARY OF CONGRESS  
Washington, DC

In The Matter of )  
 ) Docket No. RM 2008-8  
Exemption to Prohibition On )  
Circumvention Of Copyright Protection )  
Systems For Access Control Technologies )  
To: The Copyright Office )

**RESPONSES OF VIRGIN MOBILE USA, L.P.  
TO COPYRIGHT OFFICE QUESTIONS, DATED JUNE 23, 2009**

Submitted by:  
Peter Lurie  
General Counsel & Co-founder  
Virgin Mobile USA, L.P.  
10 Independence Boulevard  
Warren, NJ 07059

July 13, 2009

Virgin Mobile USA (“VMU”) concurs with CTIA – The Wireless Association ‘s (“CTIA’s”) responses to each of the questions posed by the U.S. Copyright Office in its letter dated June 23, 2009 to the hearing witnesses, including CTIA and VMU. VMU is providing supplementary responses to questions 1 and 2, in so far as they relate to or are specifically addressed to VMU. In addition, VMU is responding herewith to the Copyright Office's question in the May 1, 2009 hearing regarding the compromise proposal submitted by CTIA.

**I. Question 1:**

VMU 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?

**Response to Question #1:**

VMU is not aware of any chipsets and DRM solutions that could be utilized in its handsets to protect individual content files without incurring significant engineering, technology and development costs, such that it would be forced to considerably increase the price of its

handsets or service. Nor is VMU is aware of any other technological protection measures ("TPMs") that it could effectively use on its handsets and at the same time control costs.<sup>1</sup>

VMU testified that it is more cost-effective to use a single technological security measure to prevent access to the Embedded File System (where copyrighted materials are located) and to limit the device to a single network service. Specifically, VMU testified that because it targets lower income consumers, it develops and sells handsets at very low costs, and the types of chipsets that are used in its handsets generally "do not support [the] kind of extensive Digital Rights Management software or any kind of protection mechanisms that are outside of the industry-standard MSL mechanism."<sup>2</sup>

In this regard, we note that a third of VMU's customers are from households with less than \$35,000 in annual income, and VMU sells devices with retail prices as low as \$10-15, far below its wholesale and development costs, with the result that VMU incurs significant losses on the sale of each device. The company believes that in order to control its costs and provide handsets in conjunction with its prepaid services at prices that are affordable to lower income consumers, it is necessary to limit the number of TPMs, and associated hardware and development costs, on those handsets. An increase of just \$10 in development costs necessary for a more advanced DRM system or chipset could double the retail price of a handset and place it out of reach for many individuals. In lieu of rising handset prices, VMU's only alternative

---

<sup>1</sup> VMU also uses hardware-based measures to prevent hacking on some of its handsets, as Mr. Buerger stated in his testimony. (Testimony of C. Buerger, May 1, 2009, at 200, lines 9-11 (testimony cut-off). VMU has disabled the hardware communications port (*e.g.*, to prevent a USB connection) on some handsets, which prevents hackers from being able to upload new software onto the handset, as required to completely reflash a handset, and from downloading or transferring of software and content from the handsets. This is not an ideal solution and it makes it difficult to repair the mobile phones, but VMU has deemed it necessary in light of the exemption and the consequent risks to its investment in handsets, which would be lost if the devices were not activated with the VMU service.

<sup>2</sup> (Testimony of C. Buerger at 136, lines 6-11.)

would be to increase charges for voice and messaging services, which would effectively constrain usage by lower income customers.

As technology improves and costs decline, the ability to deploy DRM protection for specific content on a less expensive chipset may be technologically feasible for some content, but that would not itself make DRM an affordable option for VMU's lower cost handsets. Chipset availability and prices are not by any means the sole factor in determining whether a particular technological protection is cost-effective. The development and deployment costs associated with an enhanced DRM system are quite high and would significantly increase the retail costs of handsets. In addition to chip costs, significant work would be required to enable DRM in the file system and integrate it with various parts of the device, and the backend system would have to be modified to support encryption of DRM content. This would involve significant direct and indirect engineering and other costs.

As Mr. Buerger explained, "it's going to be an engineering problem. If you put enough engineers on it, you could probably resolve it over time. But it's the cost of the chip and the cost of the engineering effort that would raise -- or, have an economic impact on our business."<sup>3</sup> The point is that even where it is possible to develop separate DRM for content, the solutions require significant investments, raising the company's costs and increasing the price of handsets to the point that they become unaffordable to VMU's customer segment, individuals for whom there may be no other readily available affordable handset options.

Moreover, even on handsets that do support content-specific DRM, the protection of Java applications, ringtones, wallpaper, screensavers, etc. is complex and costly to administer. Separate DRM is required for each item of content, and its use can diminish the functionality of

---

<sup>3</sup> (Testimony of C. Buerger at 201, lines 3-8.)

other features of the handset, for instance, by draining battery power. And even then, it is not technically feasible to protect all of the valuable content on the handset using DRM. As Mr. Buerger testified, DRM technologies are only available for mobile handsets for a limited number of content types, namely certain audio and video files.<sup>4</sup>

VMU notes that the phrasing of this question suggests some confusion about the way that the Master Subscriber Locks ("MSL") works. The MSL is not a separate technological measure; it protects access to the software and contents on the handset as a whole. As described in VMU's original written submission, the MSL is equivalent to a front door lock.<sup>5</sup> DRM, when used, is a way to lock down individual items in the house. It is equivalent to putting valuable contents of a house in a safe inside the locked house. There is no reason that VMU or any other carrier should be forced to lock up all of the contents in this way, as well as lock the front door.

In any event, the question of whether or not it is technologically possible to use separate technological measure for firmware and other software and content is inapposite to this proceeding. Section 1201 does not require multiple layers of protection measures or the use of any particular TPM. It certainly does not require the use of the most sophisticated and/or expensive TPM solutions – costs that would eventually be borne by the consumer.<sup>6</sup> It merely requires that the TPMs be "effective."

There is also nothing in section 1201 that requires TPMs that are most convenient to consumers. Indeed, the Register has consistently recommended against adopting exemptions

---

<sup>4</sup> (*Id.* at 136, lines 12-23.)

<sup>5</sup> (Comments of Virgin Mobile, USA, L.P., dated Feb. 2, 2009, at 28. )

<sup>6</sup> (*See* Testimony of S. Metalitz, May 1, 2009, at 222, lines 10-14.)

based on the convenience to consumers.<sup>7</sup> Owners of copyrighted works and the distributors/licenseses of the works are free to permit the consumer to make certain uses and not others. As the Register of Copyrights stated in her 2006 Recommendation:

An exemption is not warranted simply because some uses are unavailable in the particular manner that a user seeks to make the use, when other options are available.<sup>8</sup>

In this case, the proponents seek to use the software contained in handsets on networks other than the handsets for which they were designed and sold. Moreover, the use sought to be made is not even a lawful one – it violates the express terms of the customer agreements. The fact that consumers and third party service providers desire to use the handsets and embedded software on a service other than that for which they are sold is not a sufficient reason to permit circumvention of the MSL. There are plenty of handsets available for use on other networks that (i) are sold specifically for use on such networks or (ii) are sold unlocked for use on any compatible network, either because they are not subsidized or, if subsidized, are sold in connection with a binding long-term commitment to use the service. If the exemption remains in place and VMU is not able to enforce the locks on its handsets and stay ahead of the hackers, its prepaid customers -- who tend to have lower incomes than those selecting traditional wireless plans -- would bear higher handset prices, all for the purpose of allowing a small subset of customers the freedom to activate a device with any service.

---

<sup>7</sup> See e.g., the Register's discussion of the proposed exemptions for space-shifting, DVDs that cannot be viewed on Linux operating systems and Region coded DVDs in *Recommendation of the Register of Copyright in RM 2005-11; Rulemaking on Exemptions from Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies* at 71, 74 and 75-6 (hereinafter, "2006 Recommendation") (Nov. 17, 2006), available at [http://www.copyright.gov/1201/docs/1201\\_recommendation.pdf](http://www.copyright.gov/1201/docs/1201_recommendation.pdf).

<sup>8</sup> *Id.* at 74.

In short, there is no precedent for the Copyright Office recommending an exemption that would permit circumvention of a technological measure simply because additional TPMs are available on the market, albeit at significantly higher prices.

## **II. Question 2:**

At the hearing in Palo Alto, representatives of Virgin Mobile USA stated that more information would be supplied to the Register in regard to the following question:

MR. CARSON: Which of your exclusive rights under Section 106 of Title 17 of the U.S. Code are being infringed when the customer takes that handset, switches to another service and uses the user interface, listens to the ring tones, whatever?

### **Response to Question #2:**

#### Summary of Response

As described in VMU's written submission,<sup>9</sup> the use of a VMU handset after it has been unlocked necessarily entails infringing reproductions of software on the handset. Any use of the handset requires copies to be made of the operating system in RAM. These copies are not authorized under the terms and conditions for use of a VMU handset. Use of a VMU handset on another network, or after it has been altered, is in direct violation of the terms and condition for using the handset, and clearly exceeds the scope of the license to the software and content on the handset. As described below, Section 117 does not apply to permit this use.

#### Copies made in RAM

The reproduction right in the operating system and other software on a VMU handset is infringed when a customer unlocks the handset and uses it with another carrier. The software on the handsets is licensed to the customer. The handsets cannot be used without using the

---

<sup>9</sup> (Comments of Virgin Mobile, USA, L.P., dated Feb. 2, 2009, at 18-19. )

operating system, and use of the operating system entails making copies of it in RAM. Use of any other application or content on the handset also entails making copies. When the customer unlocks the handset (without reflashing the entire operating system) and continues to use software on the handset, he or she is making reproductions that exceed the scope of its license to the software. As described below, those reproductions are in clear violation of VMU's Terms of Service, and, accordingly, are infringing.

The customized operating system, software applications and most content reside on flash memory built into the handsets. Some content (such as user generated pictures, videos, music, etc.) may reside on removable memory such as a microSD card. When the operating system and/or applications are being used on the handset, instructions embodied in such software are first copied from the flash memory into a faster memory chip, namely the RAM (or random access memory). The instructions are then loaded from RAM into the processor, where they are executed. Accordingly, any use of the handset necessarily requires making one or more internal copies of the operating system and/or applications. Likewise, in order to use any content, such content must be temporarily copied from flash memory, whether built into the handset or removable memory, into RAM. For example, in order to play a ringtone, the data representing the ringtone must be copied from flash memory into RAM.

Unless the person using the handset and making the copies has an express or implied license to do so, or an exception applies, those copies are infringing.

#### Such Copying Violates Terms of Use and Exceeds the License

As described in VMU's written submission, VMU handsets and service are provided with "Terms of Purchase" and "Terms of Service" that set out the terms and conditions for their use. The customer assents to these terms in buying the handset and using the service, respectively. These terms, which are binding contracts, limit use of VMU handsets and preloaded software to

the VMU service. Any use that implicates copyright in the software and exceeds the permission in the terms of use is infringing.

The handsets are sold in packaging that contains “Terms of Purchase” on the outside of the packaging. The customer agrees upon purchase, based on these terms on the packaging, not to alter the hardware or software on the handset and to only use the handset with VMU. The current terms used in connection with some, but not all handsets, expressly provides a license to pre-loaded software and content and provides that any use that exceeds the authorized use is infringing.<sup>10</sup>

A separate “Terms of Service” is agreed to for use of the handsets on the VMU wireless service. These terms also require that customers agree not to alter the hardware or software on the handsets and to only use VMU handsets with VMU service. To avoid any doubt, VMU's current Terms of Service expressly provide that the license to "use this software and content solely in connection with your use of the [VMU] phone on [the VMU] network as expressly authorized under these Terms of Service" shall terminate immediately upon a violation of the Terms of Service, and that any continued use of the software and content will constitute copyright infringement.<sup>11</sup>

---

<sup>10</sup> The terms on the packaging for new handsets provides: "You are permitted to use the software and content on this Virgin Mobile phone solely in connection with your use of the phone on our network expressly authorized by Virgin Mobile. Any use that exceeds this authorized use may infringe the rights of virgin mobile or its business partners. This phone is sold exclusively for use with service that Virgin Mobile USA provides."

<sup>11</sup> Specifically, the Terms of Service provide: "The software and content on the Virgin Mobile phones and devices, including the operating system, applications, data, information, music, games, images, text and other material, are owned by Virgin Mobile and/or its business partners. You are permitted to use this software and content solely in connection with your use of the Virgin Mobile phone on our network as expressly authorized under these Terms of Service. You may not distribute or upload any pre-loaded software or content to another device or transmit or broadcast the software or content, or otherwise copy or use the software or content in any manner not expressly authorized under these Terms of Service or, with respect to any downloaded content or applications, any other governing terms of use. If you violate any material term of these Terms of Service, including without limitation by using a Virgin Mobile phone or device on another network, by modifying any hardware or software on a Virgin Mobile phone or device, or by distributing, copying or otherwise using any of the software or content on a Virgin Mobile phone in a manner that is not authorized by these Terms of Service,

These Terms of Purchase and Terms of Service are enforceable contracts under the law. Courts have consistently upheld the enforceability of similar terms located on a product's packaging (like the Terms of Purchase) or within it (like the Terms of Service), or on a website (such as on VMU's website).<sup>12</sup> Such "shrinkwrap," "box-top," "browsewrap," or "clickwrap" agreements are valid and enforceable under the applicable law of various jurisdictions, especially where, as here, the purchaser or user is made aware of the terms and assents through some conduct, including the use or purchase of the product or service and failure to return a product.<sup>13</sup> VMU's Terms of Purchase and Terms of Service are classic examples of these types of agreements held enforceable by courts.

---

your license to the software and content shall terminate immediately and your continued use thereof will constitute copyright infringement." Virgin Mobile USA, L.P., Terms of Service (Telecommunications Services), <http://web.virginmobileusa.com/about/terms-and-conditions> (last visited July 13, 2009).

<sup>12</sup> See, e.g., *Hill v. Gateway 2000, Inc.*, 105 F.3d 1147, 1149 (7th Cir. 1997) ("Practical considerations support allowing vendors to enclose the full legal terms with their products."); *Ariz. Cartridge Remanufacturers Ass'n v. Lexmark Int'l, Inc.*, 421 F.3d 981, 987-88 (9th Cir. 2005) (applying California law to enforce terms on product packaging limiting the post-sale use of printer cartridges); *Moore v. Microsoft Corp.*, 741 N.Y.S.2d 91, 92 (N.Y. App. Div. 2002) (finding terms enforceable where user had an opportunity to read the license before being required to assent to terms); *Brower v. Gateway 2000, Inc.*, 676 N.Y.S.2d 569, 571-73 (N.Y. App. Div. 1998) (finding terms in packing materials of products ordered by telephone or mail enforceable); *Recursion Software, Inc. v. Interactive Intelligence, Inc.*, 425 F. Supp. 2d 756, 781-83 (N.D. Tex. 2006) (following courts in other jurisdictions in holding that clickwrap and shrinkwrap agreements are valid and enforceable); *RealPage, Inc. v. EPS, Inc.*, 560 F. Supp. 2d 539, 545 (E.D. Tex. 2007) (explaining that "Texas law recognizes the validity of clickwrap agreements"); *Sw. Airlines Co. v. BoardFirst, L.L.C.*, No. 3:06-CV-0891-B, 2007 U.S. Dist. LEXIS 96230, at \*15-16 (N.D. Tex. Sept. 12, 2007) (referencing the enforceability of a browsewrap license where website users have "actual or constructive knowledge of a site's terms and conditions").

<sup>13</sup> See, e.g., *Hill*, 105 F.3d at 1148-49; *ProCD, Inc. v. Zeidenberg*, 86 F.3d 1447, 1451 (7th Cir. 1996); *Moore*, 741 N.Y.S.2d at 92.

Indeed, courts have already found VMU's terms to be enforceable.<sup>14</sup> VMU conspicuously notifies customers in all-capital letters on the handset packaging that the purchase and use of VMU-branded wireless handsets are subject to certain restrictions, including that (1) the customer may not alter any hardware or software in the handset, and (2) the customer may use the handset only on the VMU Service. In addition, the first page of the "Terms of Service" booklet provided inside the packaging reiterates the prohibition against re-flashing. Moreover, those customers who purchase and/or activate their handsets on VMU's website must affirmatively click a box acknowledging that they agree to be bound by the Terms of Service. VMU handset customers have at least two, and in some cases three, opportunities to either not purchase or to return VMU handsets if they object to the Terms of Purchase or Terms of Service. There is nothing unusual, objectionable, or unenforceable in VMU's Terms of Purchase or Terms of Service. As such, they are enforceable agreements.

### Section 117

Section 117<sup>15</sup> is not applicable here, contrary to the Electronic Frontier Foundation's arguments in its testimony.<sup>16</sup> VMU has already addressed the inapplicability of section 117, as

---

<sup>14</sup> Courts have recognized the validity or likely validity of Virgin Mobile's contractual terms in several cases. *See, e.g., Ballas v. Virgin Media, Inc.*, 856 N.Y.S.2d 22 (Sup. Ct. 2007) (table decision) *text available at* 2007 WL 4532509, at \*3; *Virgin Mobile USA, LLC v. Trade Vision, Inc.*, No. H-06-cv-2960, at \*10 (S.D. Tex. Nov. 28, 2006) (granting Virgin Mobile's preliminary injunction and noting that "purchase of [Virgin Mobile-branded handsets] is expressly conditioned on the fact that the handsets will not be hacked or tampered with . . . and will not be used on wireless services other than the Virgin Mobile USA Service. Such prohibitions are valid and binding."); *Virgin Mobile USA, LLC v. Blue Oceans Distrib., LLC*, No. CV06-511-S-EJL, 2007 U.S. Dist. LEXIS 10783, at \*11-12 (D. Idaho Feb. 14, 2007) (noting in connection with a preliminary injunction ruling that Virgin Mobile demonstrated a likelihood of success that its packaging terms are enforceable). Similarly, the Southern District of Florida recently held that nearly identical terms and conditions located on and inside the packaging of another wireless company's prepaid phones were valid and enforceable against re-flashers. *TracFone Wireless, Inc. v. Bitcell Corp.*, No. 07-22249-CIV, 2008 U.S. Dist. LEXIS 41955, at \*3 (S.D. Fla. May 23, 2008).

<sup>15</sup> 17 U.S.C. § 117.

<sup>16</sup> (Testimony of J. Granick, May 1, 2009 at 150-51, 173-74 & 216-217.)

well as fair use, in its original written comments,<sup>17</sup> and refers the Copyright Office to those comments, but wishes to clarify several issues related to section 117 that were raised in the testimony.

Section 117 provides that an owner of a copy of a computer program may make or authorize the making of another copy or adaptation, provided that such a new copy or adaptation is created as an essential step in the utilization of the computer program. As such, in order for section 117 to apply, both of the following must be true: (1) the person making the copy must be the owner, as opposed to a licensee, of the copy and (2) the copy must be an "essential step" to the intended utilization of the software. Neither of these conditions is met in the case of use of a VMU handset after it has been unlocked and is being used with another service provider.

The CONTU report, which is typically considered legislative history of section 117, defines an "essential" step as one that is necessary to enable the use for which it was both sold and purchased.<sup>18</sup> Case law has confirmed this understanding: an essential step for purposes of section 117 is one that is necessary to permit the software to function as intended by the creator of the software.<sup>19</sup>

VMU's handsets are designed and sold for use on the VMU service. Like other carriers, VMU's handsets are customized for VMU and include VMU trademarks and copyrightable software and content. The handsets are specifically designed to be used on the VMU service and

---

<sup>17</sup> (Comments of Virgin Mobile, USA, L.P., dated Feb. 2, 2009, at 19-24.)

<sup>18</sup> Final Report of the National Commission on New Technological Uses of Copyrighted Works at 13 (1979) (hereinafter, "The CONTU Report"), *available at* <http://digital-law-online.info/CONTU/PDF/Chapter3.pdf> (*see* Comments of Virgin Mobile, USA, L.P., date February 2, 2009, at 20, n. 38.

<sup>19</sup> *See Krause v. Titleserv, Inc.*, 402 F.3d 119, 125-26 (2d Cir. 2005); *Madison River Mgmt. Co. v. Bus. Mgmt. Software Corp.*, 387 F. Supp. 2d. 521, 537-538 M.D.N.C. 2005) (noting that "it is only a copy made by the very act of installing a program into a computer that is privileged" by § 117(a)(1) and finding that the alleged infringer could make use of the software without copying the copyrighted database); *Micro-Sparc, Inc. v. Amtype Corp.*, 592 F. Supp. 33, 35 (D. Mass. 1984) (holding that the permission to copy in § 117(a)(1) is strictly limited to inputting programs).

not on other services. Any copies of pre-loaded software made in the course of use of a handset in connection with another service are not essential to enable the handset to function, as intended, on VMU's service.

The *Krause* case does not lead to a different result. The circumstances in *Krause* were entirely different from the facts at issue here. In *Krause*, a company hired an individual contractor to create a number of computer software programs intended exclusively for its business and that were key to running its business. Though the company and the contractor were negotiating an assignment of the programs, it was never executed and the consultant quit before assigning the copyrights. The company was left only with the installed copies. The software was designed in such a way that it could not be used as intended without modifications: "Many routine functions such as the addition of a new customer or change of a customer address could be performed only by changing the source code."<sup>20</sup> In other words, in order to continue using the program exactly in the way it was designed to be used by the developer, the company had to be able to modify it. The Second Circuit held that these adaptations were covered under section 117 because they were necessary to utilize the program in the very manner the software was intended to be used.

Continued use of software in clear contradiction of the agreement and scope of the permitted use cannot be said to be a use for which it was intended. This situation is entirely different from that in *Krause*. Here, customers do not need to make any copies or modifications if the handset is used as intended -- with VMU's service. It is simply not correct to say that VMU handsets are designed to be used on other services when they are specifically customized for use with the VMU service.

---

<sup>20</sup> *Krause*, 402 F.3d at 121.

Second, the handset purchasers are not owners of the software for purposes of section 117. This alone prevents reliance on section 117. Ownership is not determined according to whether or not one owns the device on which the software resides nor on title alone, but depends on whether the party "exercises sufficient incidents of ownership."<sup>21</sup>

The case law makes it very clear that software that is purchased with contractual limitations on its use is not sold, but is licensed.<sup>22</sup> In *DSC Communications Corp. v. Pulse Communications, Inc.*,<sup>23</sup> the Federal Circuit explained that the possessor of a copy is not an owner for purposes of section 117 where an agreement prohibits the possessor of the copy from using the software other than as provided by the copyright holder. In that case, the licensee was limited to use of the software "solely in conjunction with the Material [*i.e.*, the Lifespan-2000 and related equipment] during the useful life of the Material."<sup>24</sup> This is exactly the case here: a customer purchasing a handset is permitted to use the software preloaded on the handset only in connection with a particular service and is not allowed to alter it in any way, among other limitations, and thus the handset purchaser is not an "owner" of the software for purposes of section 117.

In this case, a review of the factors clearly weighs against a finding of ownership. The situation here cannot be compared to *Krause* where the software was created expressly for the company. As previously noted, VMU customers pay as little as \$10 for the handsets, the

---

<sup>21</sup> *Krause*, 402 F.3d at 124.

<sup>22</sup> See *DSC Commc'ns Corp. v. Pulse Commc'ns, Inc.*, 170 F.3d 1354, 1360 (Fed. Cir. 1999) (agreeing with non-ownership holdings in *MAI Sys. Corp. v. Peak Computer, Inc.*, 991 F.2d 511, 518 (9th Cir. 1993) and *Advanced Computer Servs. of Mich. v. MAI Sys. Corp.*, 845 F. Supp. 356, 367 (E.D. Va. 1994)).

<sup>23</sup> *DSC Commc'ns Corp.*, 170 F.3d at 1360-62.

<sup>24</sup> *DSC Commc'ns Corp.*, 170 F.3d at 1361.

software is not developed specifically for any customer, and most importantly, there are significant restrictions on use.

### Conclusion

Mobile handsets are increasingly sophisticated mobile computing devices. They are capable of performing a vast array of tasks and storing and playing large amounts of various kinds of content. Like any computer, the handsets run on complex copyrighted operating systems and contain highly creative software applications and content, just as deserving of protection as any computer software. Investments in further creative development of software are supported by the ability to sell the software in quantity. In this case, the ability to sell the software in quantity is dependent on the ability to sell the handsets in quantity and generate revenues from usage, which in turn is dependent on the ability to lock the handsets.

Similarly, when a computer is purchased, it comes bundled with some operating software and basic applications. That software is generally licensed, not owned. A mobile handset is no different: it contains operating software and applications that are licensed to the customer. The purchaser of a handset should not be permitted to use the software on a handset in violation of the license terms any more than the purchaser of a computer should be permitted to use a copy of "Windows" or "Mac OS" in a manner that violates and/or exceeds the scope of the license.

### **III. CTIA Compromise Proposal**

At the May 1<sup>st</sup> hearing, the panel asked VMU what it "thought about" the CTIA proposed compromise exemption and whether it "had anything to add."<sup>25</sup> VMU stated that it would submit a written response with its view.<sup>26</sup>

In its written submission, CTIA stated that it would not oppose the following exemption:

---

<sup>25</sup> (B. Golant, May 1, 2009 Hearing, at 178-79.)

<sup>26</sup> (Testimony of P. Lurie, May 1, at 178-79.)

Computer programs in the form of firmware in wireless telephone handsets that restrict the handset from connecting to a wireless telephone communications network, when circumvention is accomplished by an individual customer of a wireless service provider for the sole noncommercial purpose, and with the sole effect, of lawfully connecting to a wireless telephone communications network or service other than that of the service provider, provided that (i) the individual complies with all of his or her contractual obligations to the service provider, and (ii) the individual does not thereby obtain access to works protected under this title beyond those necessary to connect to such a network or service.<sup>27</sup>

VMU does not believe any exemption is warranted because the proponents have not met their burden of proof for an exemption. As a practical matter, however, VMU would not oppose an exemption that contains each of the above conditions, including without limitation, that the circumvention is limited to an individual customer for the sole noncommercial purpose and effect of connecting to a wireless telephone communications network, and the individual is in compliance with all terms and conditions of service and does not obtain access to copyrighted works other than those necessary to connect to another network or service.

VMU would like to clarify two of the conditions set out in the CTIA proposal. First, it prefers that the exemption use the language "complies with all of the service providers' terms of use of the handset" rather than "complies with all of his or her contractual obligations to the service provider" to avoid any misunderstanding among customers that the terms of use are not "contractual obligations." VMU is also concerned that there may be some ambiguity in the last clause of the proposed exemption: "the individual does not thereby obtain access to works protected under this title beyond those necessary to connect to such a network or service." The intention is to prohibit use of the exemption in any circumstances where unlocking the handset for purposes of connecting to another carrier also unlocks copyrightable software or content." Whether or not a customer thereby actually accesses any software or content on the handset

---

<sup>27</sup> (Comments of CTIA – The Wireless Association, dated Feb. 2, 2009, at 44.)

should not be a factor; rather, the question is whether the technological measure for such copyrighted works is circumvented. Any exemption should clearly state that unlocking a mobile handset is only permitted if doing so does not also unlock technological measures that control access to any copyrightable works and thereby make them available for copying, downloading or modifications or any other copyright use.

Although VMU is willing to agree to an exemption that includes each of the above limitations, VMU reiterates that the proponents of the proposed exemptions 5B, C and D (and the unified proposal) simply have not met their burden for any exemption.<sup>28</sup>

VMU appreciates the opportunity to have participated in this proceeding.

---

<sup>28</sup> The proponents' failure to meet their burden on a number of issues is described in detail in VMU's initial written comments. (*See generally* Comments of Virgin Mobile, USA, L.P., dated Feb. 2, 2009; *see also* Comments of CTIA – The Wireless Association, dated Feb. 2, 2009. )