Before the

U.S. COPYRIGHT OFFICE

LIBRARY OF CONGRESS

In the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies

Docket No. RM 2011-7

Reply Comments of the Software Freedom Law Center

March 2, 2012

Submitted by:
Aaron Williamson
Software Freedom Law Center
1995 Broadway, 17th Floor
New York, NY 10023
(212) 580-0800
(212) 580-0898 (fax)
aaronw@softwarefreedom.org

I. Introduction and summary of argument

In our initial comments, the Software Freedom Law Center voiced a self-evident proposition: the owner of a computer should decide what software to run on it, regardless of the form that computer embodies.[1] This proposal was echoed by the subsequent comments of dozens of organizations and individuals,[2] for whose unsolicited support we are deeply grateful.

Against common sense and public opinion stands a single submission, the comments a group of content industry associations who represent neither the manufacturers producing computing devices nor the users who buy them.[3] Where we affirm the right of device owners to improve

1 Software Freedom Law Center, Comment in the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies, at 2 [*hereinafter* SFLC Comments] (proposing an exemption for "[c]omputer programs that enable the installation and execution of lawfully obtained software on a personal computing device, where circumvention is performed by or at the request of the device's owner.").

2 *See* U.S. Copyright Office—Comments on Classes of Works, http://www.copyright.gov/1201/2012/comments/ (listing nearly 300 comments in support of SFLC's proposed exemption).

3 Association of American Publishers, et al., Joint Comments in the Matter of Exemption to Prohibition on

their devices, accommodate the needs of disabled persons, and ensure their own security, these groups respond with a single nonsequitur: a concern for copyright infringement that the exemption would neither enable nor encourage.

The red herring of "piracy" obscures the respondent's true purpose, to control the secondary market in operating systems and applications. They do not make this purpose explicit because it is baldly anticompetitive: as the Federal Circuit warned[4] and the Ninth Circuit acknowledged,[5] the content industry's reading of 17 U.S.C. § 1201(a) "would allow companies to leverage their sales into aftermarket monopolies, in potential violation of antitrust law."[6] Their comments in this rulemaking would themselves implicate antitrust laws were they not shielded by the Noerr-Pennington doctrine.[7]

When the Digital Millennium Copyright Act's anticircumvention provisions were first enacted, respondents reaped a windfall. The law gave them an effective power of prior restraint, presumptively banning all manner of lawful activity where technological protection measures were used. It is no surprise, then, that they have never met an exemption that they didn't oppose —here, they call even limited accommodations for blind and deaf persons "unnecessary."[8] They should not be allowed to extend their already-substantial control to copyrighted software produced by others.

SFLC's exemption would have neither the legal nor the practical effect of encouraging infringement; rather, it would protect innovation in the secondary market, promoting the production of new copyrighted works and the security of users. DMCA § 1201(a)(1) is concerned with unauthorized copying of copyrighted works. But where, as here, it is used not to prevent infringement but to control the secondary market in computing hardware or software, its reach must be curtailed.

II. The proposed exemption promotes innovation, not infringement

A secondary software market for computing devices promotes the improvement of technology for social benefit. Where devices that customers already own are controlled by powerful vendors, innovation is limited by the vendors' imagination and financial interests. Independent control of devices enables independent development and also individual freedom: free software allows persons with disabilities and their allies to make software (and the hardware it runs on) more accessible.[9] SFLC's exemption would enable independent accessibility work on all devices, not only at the application but at the operating system level.

An independent secondary market is also essential to software security. The locked-down model

---

Circumvention of Copyright Protection Systems for Access Control Technologies [*hereinafter* Content Industry Comments].

4 Chamberlain Group, Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1193 (Fed. Cir. 2004).

5 MDY Indus., LLC v. Blizzard Entm't, Inc., 2011 U.S. App. LEXIS 3428, at *49 (9th Cir. 2011).

6 *Id*.

7 E. R.R. Presidents Conference v. Noerr Motor Freight, Inc., 365 U.S. 127, 135 (1961).

8 Content Industry Comments at 43.

9 To give just one example, the Eyes-Free project adapts free software to accommodate users with vision disabilities. Google Code—Eyes-Free, https://code.google.com/p/eyes-free/.

promoted by the content industry puts mobile phone users' security in the hands of mobile network carriers, who have all but abdicated responsibility for their customers' security. As we pointed out in our proposal, nearly every locked-down Android phone produced stops receiving security updates in the span of a year.[10] Users of unrestricted devices can patch security holes as they arise, in response to the regular reports and corresponding fixes issued by developers.[11]

The content industry insists that users cannot be allowed the freedom to improve their lot or secure their own devices, however, because someone might infringe a copyright. This criticism is an astonishingly brittle strawman—it has nothing to do with the actual exemption proposed.

A. The exemption would not enable unauthorized use or copying of applications

The thrust of the respondents' objection is the observation that some copyright owners restrict media and trial versions of applications using technological protection measures, and that people circumvent those measures for purposes of infringement.[12] While a concern for infringement is understandable in the abstract, the proposed exemption would have no practical or legal effect on infringement of copyright in applications.

The proposed exemption permits “the installation and execution of lawfully obtained software.”[13] The respondents suggest that this would undermine the use of “code signing” to limit the functionality of trial versions of applications and to prevent unauthorized copying or modification of applications.[14] Simply put, it wouldn't; it merely allows device owners to install legitimate copies of *unsigned* applications without being subject to civil liability. The Android platform demonstrates that code signing is compatible with user freedom: many Android devices both enforce code signing and permit the installation of unsigned applications.[15] The availability of unsigned applications has not reduced the prevalence or effectiveness of code signing on Android systems.

The unauthorized copying that respondents fear requires a separate step of circumvention: either removing the signature from an application or disabling enforcement of signatures in the device's software.[16] The proposed exemption does not authorize either of these circumvention techniques,

---

10 Michael Degusta, *Android Orphans: Visualizing a Sad History of Support*, theunderstatement, Oct. 26, 2011, http://theunderstatement.com/post/11982112928/android-orphans-visualizing-a-sad-history-of-support.

11 In the personal computer market, where users have until recently been relatively unrestricted, such regular updates are common for both proprietary and free software. See Wikipedia—Patch Tuesday, https://en.wikipedia.org/wiki/Patch_Tuesday (describing Microsoft's regular update process); Debian—Security Information, http://www.debian.org/security/ (describing the security practices of Debian GNU/Linux).

12 Content Industry Comments at 30.

13 SFLC Comments at 2.

14 Content Industry Comments at 30.

15 *See* Donovan Colbert, *How to side-load apps on your Android device*, TechRepublic, July 18, 2011, http://www.techrepublic.com/blog/smartphones/how-to-side-load-apps-on-your-android-device/3114; Android Developers—android.drm, https://developer.android.com/reference/android/drm/package-summary.html (describing Android's digital rights management framework).

16 *Compare* Adam Frucci, *Crackulous Allows for App Store Piracy*, Gizmodo, Feb. 2, 2009, http://gizmodo.com/5144751/crackulous-allows-for-app-store-piracy (describing Crackulous, an application that strips technological protection measures from applications purchased from the iTunes App Store), *with* Mike Keller, *JailbreakMe 3.0: How Does it Work?*, PCWorld, https://www.pcworld.com/article/235144/jailbreakme_30_how_does_it_work.html (describing JailbreakMe, an

much less establish an “open-ended standard for circumvention”; anyone who circumvents measures protecting signed applications for purposes of infringement would remain subject to liability under § 1201(a)(1) notwithstanding the exemption. Indeed, as the Electronic Frontier Foundation's comments show, circumvention of application locks has given rise to a booming alternative market for legitimate applications, producing tens of millions of dollars in licensing revenue annually for developers who are excluded from Apple's App Store.[17]

Should the slightest suspicion remain that the proposed exemption gives comfort to infringers, it cannot survive a simple reading of the exemption, which permits circumvention only for the purpose of installing *licensed* software.[18] And because the exemption would not enable infringement of any sort, respondents need not be concerned that it will expose those who install “bootleg” applications to hidden malware; application developers' reputations among willful infringers will remain safe.[19]

B. Application and operating system locks harm the market for independent alternatives across all platforms

Respondents worry that allowing purchasers of “every device and every platform” to choose what legal software they use is “premature,” enabling consumer freedom on platforms over which manufacturers and vendors have not yet asserted total control.[20] SFLC documented in our initial proposal how the operating system and application locks common on mobile phones were becoming standard across the personal computing industry.[21] Since we submitted that proposal, respondents' own members have taken concrete steps to expand their control over users to “every device and every platform,” adding ample evidence to that presented in our initial comments.

We pointed out in those comments that the next generation of personal computers will implement a new hardware-interface standard, called UEFI, that will enable manufacturers to prevent the installation of unapproved operating systems via its “secure boot” system. We argued that operating system vendors will likely use this new capability to enforce operating system locks on personal computers, just as on mobile devices.[22] What was then likely has since become fact. Two weeks after we submitted our proposal, Microsoft (a member of the Business Software Alliance, one of the respondents) published a new policy that mandates operating system locks for a range of devices that is broad to the point of being indeterminate.[23]

---

application that enables the installation of unsigned applications on iOS).

17 Comments of the Electronic Frontier Foundation in the Matter of Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies , at 10 [*hereinafter* EFF Comments].

18 In their reply to EFF, respondents argue that if exemptions are not limited to circumvention for the “*sole* purpose” of installing licensed software, they would somehow legitimize circumvention for the purpose of copyright infringement, so long as the circumvention and the infringement were separated by a single exempt act. That anyone could escape liability under § 1201(a)(1) under such circumstances defies credibility. Nonetheless, the Register could easily qualify any recommended exemption to exclude this unlikely outcome.

19 *See* Content Industry Comments at 31 (worrying that “malicious developers often insert malware within such pirated applications” and might cause “consumers... to mistrust their applications.”).

20 *Id*.

21 SFLC Comments at 3–10.

22 *Id*.

23 Microsoft, Windows Hardware Certification Requirements: Client and Server Systems, Dec. 2011, http://download.microsoft.com/download/A/D/F/ADF5BEDE-C0FB-4CC0-A3E1-B38093F50BA1/windows8-

This policy requires any manufacturer of a Windows-certified device to lock out unauthorized operating systems using UEFI secure boot if the device employs the ARM architecture.[24] This policy has implications for every class of personal computing device. Not only are the Apple iPhone and nearly every Android phone based on ARM chips, but Microsoft *requires* all Windows phones to be built upon ARM.[25] Manufacturers have already begun to produce ARM-based Windows tablet computers and, as our comments anticipated, personal computers.[26]

All of these new Windows phones, tablets, and personal computers are required by Microsoft to carry operating system locks as a precondition for certification. Worse, this policy ensures that Microsoft's restrictive policy will hamper any new platform Windows expands to. ARM is the most popular platform for nearly every class of personal computing device: not only mobile phones and tablets, but e-book readers,[27] digital cameras,[28] hand-held video game systems,[29] GPS devices,[30] and Internet-enabled televisions.[31] Respondents, in arguing that SFLC's case for the expansion of operating system locks is "speculative," conspicuously neglect their members' deliberate expansion of these restrictions to a limitless array of personal computing devices.

III. Reasonable alternatives to circumvention are not available

In response to EFF's proposed "jailbreaking" exemption for phones and tablets, respondents argue that an exemption is not necessary because "[m]obile phones and tablets running the Android operating system are available completely unlocked."[32] While this is true for these two classes of Android device (the respondents produce no support for their contention that unlocked Android e-book readers are available), it is insufficient to demonstrate that an alternative exists for phones and tablets, much less the broad range of personal computing devices to which operating system and application locks are applied.

Respondents suggest that, as an alternative to circumvention, mobile phone owners can "switch from one phone device to another."[33] They wave aside the often-prohibitive cost of such a switch with unsupported suppositions about declining future hardware prices, while pointing to a single $529 phone as proof of this supposed alternative.[34] This high price is no exception: carriers

hardware-cert-requirements-system.pdf.

24 *Id* at 116.

25 ARM—Windows Phone, http://www.arm.com/community/software-enablement/microsoft/windows-mobile.php (noting that "Windows Phone is exclusively offered on the ARM architecture.").

26 Agam Shah, *Qualcomm targets PCs, takes aim at Intel's ultrabooks*, IT World, Jan. 10, 2012, http://www.itworld.com/hardware/240039/qualcomm-targets-pcs-takes-aim-intels-ultrabooks.

27 ARM—Sony PRS500 eBook reader, http://www.arm.com/markets/mobile/sony-prs500-ebook-reader.php.

28 ARM—Casio EX-F1 Digital Camera, http://www.arm.com/markets/home/casio-ex-f1-digital-camera.php.

29 ARM—Nintendo DSi, http://www.arm.com/markets/home/nintendo-dsi.php.

30 Ray Willington, *TomTom GO LIVE 1000 Adds Capacitive Touchscreen, ARM 11 CPU*, HotHardware.com, Apr. 28, 2010, http://hothardware.com/News/TomTom-GO-LIVE-1000-Adds-Capacitive-Touchscreen-ARM-11-CPU/.

31 ARM—Sony BRAVIA KDL-32L4000 HDTV, http://www.arm.com/markets/home/sony-bravia-kdl-32l4000-hdtv.php.

32 Content Industry Comments at 22.

33 *Id*.

34 *Id.* n.35; Tim Bray, *Nexus One Developer Phone*, Aug. 5, 2010, http://android-developers.blogspot.com/2010/08/nexus-one-developer-phone.html ("As of today, the Developer Phone is the Nexus One, at a price of $529.").

simply do not offer unlocked smartphones at the subsidized prices that enable most people to afford them, effectively imposing a “freedom tax” on users who wish to avoid software restrictions. For now, we live in a world where no laptop computer manufacturer could say to its customers with a straight face, “Buy a computer from someone else if you want to install your own software.” Such a policy is no more acceptable for mobile phones—computers which rival laptops in both cost and functionality—or indeed for any personal computing device.

As we demonstrated in our initial comments, there are many other reasons that buying a new phone is no alternative to circumvention. The most obvious is that no platform substitutes exactly for another: mobile phone users, for example, often choose to unlock their phones to gain access to a specific application or feature that is only available on the platform they chose to begin with.[35] Other reasons we discussed include that unlocked devices can run less resource-intensive operating systems or be repurposed for other tasks. This extends the useful life of devices, supporting a secondary market for operating systems, applications, and devices, and reducing environmental waste.[36]

As operating system and application locks spread to personal computers and all other manner of computing device, many of the forces that shorten the useful life of cellphones will apply there as well. SFLC's proposed exemption will increase the utility and lifespan of all of these devices; the status quo will ensure that devices will quickly become obsolete and be discarded. While an anemic secondary market for devices would benefit the respondents' members, it would greatly harm consumers and the market for alternative operating systems.

IV. The statute does not forbid “trafficking” in aftermarket software

Finally, respondents argue that software developers to improve the software on locked-down devices would “clearly” permit “a trafficking violation.”[37] We understand that respondents would like § 1201(a) to prohibit “trafficking” in anyone's software but theirs, but thankfully it does not, nor should it give them power to exclude software they did not produce from devices they do not own.

V. Conclusion

Competition and innovation in software depend upon a free secondary market. The Librarian can enable both, contrary to respondents' parsimonious view of the Librarian's authority.[38] And he can do so without the least effect on respondents' legitimate interests. We urge the Register to recommend SFLC's proposed exemption and allow device owners to reap the benefits of a truly competitive software market.

---

35 For example, jailbreaking the iPhone allows use of the FaceTime video chat feature over mobile data connections as well as WiFi. Brennon Slattery, PCWorld, *5 Reasons to Jailbreak Your iPhone - and 5 Reasons Not*, Aug. 3, 2010, https://www.pcworld.com/article/202441/5_reasons_to_jailbreak_your_iphone_and_5_reasons_not.html.

36 SFLC Comments at 5–8.

37 Content Industry Comments at 32.

38 In their comments, respondents describe in detail their view of the limits of the Librarian's authority and admonish the Register to be “extremely cautious about making any pronouncements on the legal issues presented,” lest she “unintentionally distort the development of copyright law.” *See* Content Industry Comments at 4–8. They offer no opinion on intentional distortions of copyright law.