Northwestern Journal of Technology and Intellectual Property

Volume 6
Issue 1 *Fall*

Article 3

Fall 2007

Caveat Venditor: Technologically Protected Subsidized Goods and the Customers Who Hack Them

Christopher Soghoian

N O R T H W E S T E R N
JOURNAL OF TECHNOLOGY
AND
INTELLECTUAL PROPERTY

Caveat Venditor: Technologically Protected Subsidized Goods and the Customers Who Hack Them

Christopher Soghoian

Fall 2007 VOL. 6, NO. 1

Northwestern Journal of Technology and Intellectual Property
Volume 6, Number 1 (Fall 2007)

Caveat Venditor: Technologically Protected Subsidized Goods and the Customers Who Hack Them

By Christopher Soghoian*

I. INTRODUCTION

¶1 This paper focuses on the subsidization of a technology-based durable good.[1] It goes on to discuss the delicate dance between the producer trying to protect its profit, competitors trying to create and sell aftermarket goods,[2] and those innovative customers who use the items in completely unplanned and unprofitable ways.

¶2 An age old, but increasingly popular business model involves the subsidization of a proprietary durable good by a manufacturer, such that the good is sold below cost.[3] Due to careful design, technological, and legal restrictions, the producer creates a primary product that is only compatible with its own aftermarket goods. It is through the sale of these proprietary aftermarket products that the producer is able to recoup its initial investment. An example of this business model may be seen with the free inkjet printers that are included with the cost of a new computer but which require proprietary ink refill cartridges that are sold at a significant markup. This business model is typically referred to as the razor and blade model, although this term is a somewhat imperfect description.[4] However, since this term is in common use, this paper will continue to use it to refer to this business model.

¶3 In economic terms, when the costs to consumers of aftermarket goods are less than the cost required to switch to a different and competing primary product, consumers are said to be "locked in" to the primary durable good and its aftermarket.[5] This "lock in"

* School of Informatics, Indiana University, Bloomington, Indiana.

[1] A durable good is a consumer good (such as vehicles and household appliances) that are typically used repeatedly over a period of years. Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/durables (last visited Nov. 7, 2007).

[2] An aftermarket is the market for parts and accessories used in the repair or enhancement of a product or a secondary market available after sales in the original market are finished. Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/aftermarket (last visited Nov. 7, 2007).

[3] An early example of this business model was used by Standard Oil in China in the early 1900s. Millions of *Mei foo* kerosene lamps were distributed at a few cents each or were given away with the first case of kerosene. *See* ExxonMobilChemical.com, *Our History in China* (2006), http://www.exxonmobilchemical.com.cn/China-English/LCW/About_ExxonMobil/Our_History_in_China.asp. The lamps "would burn [Standard Oil's] brand of kerosene to perfection but, if competing brands were used, would send up such a smoking stench that Chinese were terrified." *Far Eastern Alliance*, TIME MAGAZINE, Aug. 28, 1933, *available at* http://www.time.com/time/magazine/article/0,9171,930122,00.html.

[4] Razors are typically not sold at a loss but at a modest profit. Razor companies typically earn the majority of their profits through the sale of expensive replacement blades. As the razors are not subsidized and sold below cost, they do not truly reflect the business model that is the focus of this paper.

[5] Switching costs include not only the price of a new primary product, but also the inconvenience and

pricing strategy can fail when competitors begin to produce compatible aftermarket goods. As such, producers can be extremely protective of their markets, especially when they have subsidized the primary good and sold it at a loss.

¶4 This paper first examines a number of issues that relate to the razor and blade business model, such as:

(1) what happens when users wish to use the primary good in a way that the subsidizer had not intended and thus do not purchase the add on-services upon whose sale the seller is depending;
(2) what happens to the individual users that do this and, more importantly, those who create and distribute information telling others how to do so; and
(3) what happens to competitors who wish to introduce an aftermarket replacement good that is designed to work with another firm's subsidized primary good? Should this kind of free-riding be allowed? Is it fair that competitors can undercut the company producing the primary good, since the competitors do not need to recoup the subsidization cost?

¶5 The second part of this paper recalls a number of struggles between durable good manufacturers and their hobbyist customers. The third part of this paper goes on to present a number of legal cases that relate to companies fighting off the efforts of competitors who seek to sell aftermarket goods targeting the companies' own subsidized durable goods. Section four contains an in-depth analysis of a number of the issues that the previous sections introduced. The paper then concludes with section five.

II. THE RAZOR — CASE STUDIES

¶6 While there is a fairly significant body of legal history involving companies that try to compete in each other's aftermarkets, there is very little in the way of case history involving customers who tinker with subsidized primary goods. For the companies who develop these products, such customers are as much of a threat to the the profitability of the business model as other firms competing for their aftermarket sales. The end result is the same: an initial product is sold below cost and the company is left with no way to recoup its initial investment. Some companies have issued legal threats to these innovative customers who modify the products and, more importantly, those who share information on the modifications with others. These legal threats have not been followed up in the courts.

¶7 The majority of the following examples involve customers who reverse engineer[6] a locked-down proprietary product and discover a way for it to serve a completely different purpose, typically one that does not involve the customer purchasing any further aftermarket goods. As long as this remains a technically difficult task, it remains restricted to a small number of technically savvy users and, therefore for the most part, it

additional expenditures required to make a switch. *See* CARL SHAPIRO & HAL R. VARIAN, INFORMATION RULES: A STRATEGIC GUIDE TO THE NETWORK ECONOMY 103-04 (Harv. Bus. School 1999).

[6] Reverse engineering can be defined generally as a "fair and honest means . . . [of] starting with the known product and working backwards to divine the process which aided its development or manufacture." Kewanee Oil Co. v. Bicron Corp., 416 U.S. 470, 476 (1974).

is not a threat to the manufacturer. However, if the information is distributed in an easy to use form by hobbyists on the Internet, it can and has in past situations caused significant financial harm to those companies producing the goods.

¶8 This section now explores several instances where a proprietary product was reverse engineered by hobbyists who had little to no incentive to purchase aftermarket products. In many ways, this will be a case of David versus Goliath or open source programmers versus large corporations.

A. Microsoft's Xbox Versus The Linux Hackers

¶9 Microsoft released the Xbox video gaming system to the U.S. market in November 2001.[7] It was a much hyped and significantly expensive[8] effort to break into the console gaming market, which at the time was dominated by Sony's Playstation,[9] and, more importantly, to gain access to the living room.[10] To do this, Microsoft adopted the typical business strategy used in the console gaming business:[11] sell the hardware at a loss, control which software can run on the device, and extract a royalty fee from the makers of each game sold.[12] Microsoft hoped that it could recoup the costs of its investment through the sale of games, accessories, and other services. This proved to be a fairly risky strategy as the company is reported to have lost up to $150 on each XBox.[13]

¶10 Given the considerable investment that Microsoft had made in the Xbox product, the company had a strong incentive to be very protective of the various revenue streams through which they hoped to recoup their costs and, hopefully, make a significant profit. Microsoft foresaw a number of potential threats to the financial success of its platform,

---

[7] "Starting Nov. 8, 2001, Xbox consoles will be available for purchase at retail outlets throughout North America for an estimated retail price of $299." Press Release, Microsoft (May 16, 2001), *available at* http://www.microsoft.com/presspass/press/2001/may01/05-16xboxlaunchdetailspr.mspx.

[8] "Industry analysts have been estimating that Microsoft will have to absorb losses of $1 billion to $2 billion related to its effort to subsidize for the manufacturing of Xbox . . . . Microsoft also is investing heavily in marketing and has set aside $500 million to promote Xbox." Richard Shim, *A $500 Million Gamble*, CNET NEWS.COM, Nov. 15, 2001, http://news.com.com2009-1040-275793.html.

[9] "Since the launch [of the Xbox] on Nov. 15 [2001], about 1.5 million consoles have been sold. That beats Nintendo's GameCube, which has sold 1.2 million units since its Nov. 18 launch. Meanwhile, Sony's PlayStation 2, out since Oct. 25, 2000, sold 2.5 million units in North America this Christmas season. "While Xbox is designed first and foremost to best PlayStation 2 and GameCube, the connected-home vision is a constant undercurrent." Jay Greene et al., *Bill Gates in Your Living Room*, BUSINESS WEEK ONLINE, Jan. 21, 2002, http://www.businessweek.com/magazine/content/02_03/b3766095.htm.

[10] "With PC sales expected to decline for the second straight year as corporate spending withers, Microsoft is aiming its big guns on entertainment goodies for the home. It's spending more than $2 billion building and marketing its new Xbox game console . . . . Microsoft is counting on Xbox to jump-start its digital home initiative." *Id*.

[11] "Like other console makers, Microsoft is subsidizing the cost of the console and hoping to recover its expenses through sales of game software and the decreasing cost of components over time." Shim, *supra* note 8.

[12] "5.5 SOFTWARE TITLE LICENSE . . . . Licensee shall pay Microsoft royalties, on a Software Title-by-Software Title basis, for each Finished Product Unit manufactured . . . ." Xbox Publisher License Agreement Between Microsoft & Majesco Entertainment Co., *available at* http://www.secinfo.com/dsvrn.12Qq.d.htm#1stPage (SEC Exhibit 10.1 filed by Majesco Entertainment Co.).

[13] "As it stands, Microsoft makes a significant loss - thought to be over $150 - on each Xbox console it sells, and the Home and Entertainment Division of the company, which houses the Xbox project, regularly turns in large quarterly losses as a result." *Microsoft Pledges to Cut Xbox Costs*, THE REGISTER (UK), June 26, 2003, *available at* http://www.theregister.co.uk/2003/06/06/microsoft_pledges_to_cut_xbox/.

and thus designed a significantly complex Digital Rights Management (DRM) system which it embedded within the Xbox. It is to these potential threats that this paper now turns.

B. Region Enforcement

¶11 Price discrimination, the strategy of charging different groups of customers different prices, is a common practice in many industries.[14] It is a common practice in the video game industry to lock a consumer device to a specific region, such that games imported from another part of the world will be rejected by the gaming console. This allows game producers and distributors to exert a fine level of control over the sale of their products. Titles can be released at different times in different markets, sold for different prices, and under different licensing terms. Distributors in foreign markets can "wait and see," basing their decision to license and distribute a product based on the popularity and sales in its primary market.

¶12 A company cannot reasonably expect a software title that is sold for $50 in the United States to be successful when sold for $50 in a developing market such as China or Brazil. Recognizing that such high prices often drive customers to piracy, many firms have introduced cut-price editions of their goods to developing markets.[15] Likewise, in more expensive markets such as the United Kingdom, companies would ideally like to be

---

[14] "The cost of buying a single song across the 27-nation bloc varies among the available iTunes stores in EU nations. For example, downloading a single in Britain costs $1.56, in Denmark $1.44, while in countries using the euro such as Germany and Belgium, a single costs $1.32." Associated Press, *EU Probes Apple Over iTunes Prices*, Apr. 3, 2007, *available at* http://www.webdesignbangkok.net/news_EU_probes_Apple_iTunes.php. "[Apple] has sold songs at 99 cents per song since it introduced the [U. S.] iTunes music store in 2003, and has resisted the calls of labels to change that pricing strategy." Tom Krazit, *Apple, Labels Stick With 99 Cents Per iTunes Song*, CNET NEWS.COM, May 1, 2006, http://news.com.com/Apple,+labels+stick+with+99+cents+per+iTunes+song/2100-1026_3-6067193.html. Price discrimination is common, although difficult to enforce, in the pharmaceutical business. *See generally* Richard Hornbeck, *Price Discrimination and Smuggling of AIDS Drugs*, 5 TOPICS IN ECON. ANALYSIS & POL'Y 1404 (2005), *available at* http://ideas.repec.org/a/bep/eaptop/v5y2005i1p1404-1404.html. "The motion picture studios . . . required that [DVD] technology permit each DVD movie copy to be coded for decryption in only one of six world regions. In other words, a DVD movie that had been coded for Region 1 (U.S. & Canada), could not be decrypted and viewed by a DVD player manufactured for sale in Region 2 (Japan, Europe, South Africa, and the Middle East) . . . ." Jeff Sharp, *Coming Soon To Pay-Per-View: How The Digital Millennium Copyright Act Enables Digital Content Owners to Circumvent Educational Fair Use*, 40 AM. BUS. L.J. 1, 25-26 (2002).

[15] "[T]extbooks are printed legally in India under copyright arrangements worked out over the last decade by American and British publishers . . . . Indian companies publish the books in black-and-white, low-quality paperback editions, and sell them for as little as 10 percent of the cost of the same book in the United States. But under the licensing agreement, the books may be sold only on the Indian subcontinent and in surrounding countries — limits that are stamped on the books' covers." John O'Neil, *Getting Textbooks Cheaper From India*, N.Y. TIMES, Mar. 29, 2006, *available at* http://www.nytimes.com/2006/03/29/education/29textbooks.html. "[P]irates entered China's market because legitimate DVDs were too expensive for the average Chinese consumer, the release dates were too late, and the demand for films was higher than the available supply. Treating pirates as competitors, [Warner Home Video China] has lowered its prices, shortened the window between the theatrical release and DVD release, and offers bonus features . . . [We] released the DVD for Crazy Stone, which was priced at ¥10- ¥15 [$1.3-$1.9], two weeks after the theatrical release. Crazy Stone did very well at the box office and on DVD, and because of its quick release date and low price, we were able to outplay the pirates." Paula Miller, *Reeling in China's Movie Fans*, THE CHINA BUS. REV., Mar. 2007, *available at* http://www.chinabusinessreview.com/public/0703/miller.html.

able to sell titles for higher yet typical market rates.[16] Without effective region enforcement, this significant difference in regional pricing creates a massive incentive for merchants to engage in arbitrage, which is the importation of products from cheaper countries to those that are more expensive.[17] A difference in price is not the only reason that users would wish to import a product from abroad. Customers in foreign markets often wait significant periods for the release of titles.[18] Furthermore, many titles are deemed to have too small a market outside of the home-country. If the predicted demand for a product in one market is too low to make the cost of a release profitable, the rights' holder will not do so. Fans of obscure and foreign language releases will be left with a problem: there may not be enough potential customers to justify a legitimate release in their market, but due to the region coding scheme on the discs, an imported copy will not play.

¶13 All of these factors (price, distribution schedules, and the availability of obscure foreign titles) add up to a strong incentive for customers to find a way to work around the DRM scheme that is the backbone of region lock enforcement.

C. Hobbyist Created Games

¶14 Microsoft's business model depended on it getting a license fee from each software title that was sold for the Xbox platform. This had the unfortunate side-effect of locking out hobbyists, college students and independent software developers who wished to make games and give them away for free.

D. Linux

¶15 A version of the Linux operating system has been created for almost every platform imaginable. This includes previous console gaming systems,[19] the Apple iPod,[20] and

[16] A copy of the Guitar Hero II game and game controller for the Xbox 360 currently sells for $84.99 on Amazon.com (U. S.), while the European region edition sells for the equivalent of just over $132.84. Even including international shipping fees, without region controls, it would be cheaper for UK customers to order a copy from American online retailers. *Compare* Amazon, http://www.amazon.com (last visited Nov. 17, 2007) *with* Amazon UK, http://www.amazon.co.uk (last visited Nov. 17, 2007).

[17] "If pills cost 50 cents in Congo but $5,000 in New York City, there's a very strong incentive to jump on a plane in Congo with a bagful and resell them in New York." Lawrence Lessig, *Stop Making Pills Political Prisoners*, WIRED, Feb. 2004, *available at* http://www.wired.com/wired/archive/12.02/view.html?pg=5.

[18] "Huge delays in airing overseas TV shows locally are turning Australians into pirates, says a study conducted by technology lawyer and researcher Alex Malik. It took an average of 17 months for programs to be shown in Australia after first airing overseas . . . . These delays are one of the major factors driving Australians to use BitTorrent and other internet-based peer-to-peer programs to download programs illegally from overseas, prior to their local broadcast." Asher Moses, *TV Program Delays 'Turning Viewers Into Pirates'*, SYDNEY MORNING HERALD, Feb. 21, 2007, *available at* http://www.smh.com.au/news/home-theatre/tv-program-delays-turning-viewers-into-pirates/2007/02/20/1171733750719.html.

[19] "[Sony] announced today that it is set to release 'Linux (for PlayStation 2)' Release 1.0, targeted toward the Linux development community in North America. Designed as a hobbyist development environment, users can not only run the wide variety of computer applications written for the Linux operating system, but also create original programs and applications designed to run on [Linux] . . . ." Press Release, Sony Computer Entertainment America (May 10, 2000), *available at* http://http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=104 STORY=/www/story/01-30-2002/0001658223.

[20] *See generally* The iPodLinux Project Main Page, http://ipodlinux.org/Main_Page (last visited Nov. 7,

even a toaster oven.[21] Much of the motivation for making Linux compatible with obscure platforms is due to the "hack factor," or pleasure derived from the intellectual challenge of reverse engineering an unknown platform. The Linux operating system has its roots in the open source community, and the process of reverse engineering is one that is very familiar to many Linux developers.

¶16 The Xbox was seen as an ideal Linux platform. It was a small device, well-engineered with good hardware, and it included the ability to output video to a television. It was seen as a perfect platform for a living room Linux computer, suitable for surfing the web and watching movies from the sofa. Due to the combination of a per-device subsidy by Microsoft, as well as the economy of scale savings achieved through mass production, a hacked Xbox made for a much cheaper home media platform than building one using off-the-shelf computer components. Shortly after the launch of the Xbox, the CEO of the Lindows Linux Software company announced two prizes of $100,000 each: one to the first person to show a copy of Linux running on the Xbox and another to the first person able to run Linux on the Xbox without any hardware modifications.[22]

E. Copied Games And Backups

¶17 The final, and most high profile of the threats to the Xbox revenue stream came from those who wished to play either fair use backups of their games, or more often, illegally made copies. Previous game platforms had suffered from design flaws and clever hacks that allowed players to play such copies.[23] The majority of these hacks required so-called "mod-chips," a computer microchip that had to be invasively installed into the game console.[24] After installing one of these hacks, or modifying the game console, a user could "burn" a copy of a game to compact disc and then use that copy to play the game in the future. With video rental stores such as Blockbuster also supplying a rapidly expanding video game rental market, this meant that someone could rent a game, make a copy, return the copy, and then keep playing that game, all without the game copyright owner and Microsoft receiving the payments they were expecting. As the Xbox came with a hard disk built into the device, the threat of hacked backups was a significant one. Were Microsoft's security system compromised, users would then be able to copy games to the Xbox's hard disk and then play the games directly off the system in the future. The purchase or rental price of a single game could be spread among a group of friends. Worse, the data files for illegally copied games could be spread on the Internet for people to download en masse.

2007).

[21] *See generally* K12Linux in Schools Project: Toaster Oven Terminal Server Linux Appliance, http://web.archive.org/web/20060923005902/http://www.riverdale.k12.or.us/linux/toaster/ (last visited Nov. 17, 2007).

[22] *See generally Lindows Founder Offered Xbox Linux $200,000 Prize*, THE INQUIRER, Jan. 2, 2003, *available at* http://www.theinquirer.net/en/inquirer/news/2003/01/02/lindows-founder-offered-xbox-linux-200000-prize.

[23] *See How to Backup PSX Games*, July 18, 2001, http://www.dlc.fi/~ihra/psx_copy.htm.

[24] *See generally* Vijay G. Brijbasi, Comment, *Game Console Modification Chips: The Effect of Fair Use and The Digital Millennium Copyright Act on The Circumvention of Game Console Security Measures*, 28 NOVA L. REV. 411 (2004); *see* Andrew Leung, *Modchips on Trial*, 2003 UCLA J.L. & TECH. 24 (2003).

F. Breaking The Security Of The Xbox

¶18 Microsoft opted to protect its platform against all four of the previously described threats with one technical solution: any software that ran on the XBox needed to be "digitally signed" by Microsoft. Without a valid digital signature, the software would be rejected by the Xbox.[25] To protect its revenue, Microsoft would only issue a digital signature to those software firms that obtained a license from Microsoft and thus agreed to pay royalties.

¶19 The problem of this approach, of course, is that the four different groups, which would normally have very little in common, were now motivated to share information and target the one security system holding them back. While those users who wished to play illegal copies of games were motivated by their desire to avoid paying for software, the other three groups had more personal motivations: creativity, and the desire to do what they felt was their right. Furthermore, both the Linux community and the hobbyist game developer community include skilled and motivated programmers — who by definition — spend their time working on projects for free. In creating a single DRM system, Microsoft inadvertently aligned the "software pirates" with a team of skilled open-source programmers with significant experience in reverse engineering proprietary systems. This is the very same design mistake that was made by the creators of the DVD DRM system.[26]

¶20 The first breach of Microsoft's DRM came from the mod-chip community, but did not pose a significant threat to Microsoft due to the difficult process that installing such a chip required.[27] In July of 2003, the Free-X project announced that its members had figured out a way to get Linux running on the XBox without any hardware modifications.[28] The developers were able to exploit a flaw in one of the system's games using a "buffer overflow," a technique commonly used in the computer security community.[29] Once they had successfully created a software-based hack, the Linux developers gave Microsoft an ultimatum: release a digital signature for the Linux

---

[25] *See generally* Michael Steil, *17 Mistakes Microsoft Made in the Xbox Security System*, Oct. 25, 2005, http://www.xbox-linux.org/wiki/17_Mistakes_Microsoft_Made_in_the_Xbox_Security_System.

[26] The groups wishing to break the DVD DRM system consisted of: those wishing to play imported DVDs from other regions, those wishing to make copies of DVDs either for backup or "piracy," and those wishing to play DVDs on the Linux operating system. It was a Linux programmer who released the first program to break the DVD DRM system, DeCSS, although his efforts provided spill-over benefits to those other interested parties. *See generally* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp 2d 294 (S.D.N.Y. 2000), *aff'd sub nom*. Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

[27] "The Xtender, a 'mod chip' intended to be added to the main circuit board of the Xbox, went on sale last weekend . . . . Most of the mod chips promise similar functions based on disabling copy-protection features built into the Xbox. Customers are promised the ability to play games copied on recordable CD and DVD discs (and perhaps swapped as files on the Internet), play otherwise inaccessible foreign titles, and copy DVD movie discs otherwise protected by software from Macrovision . . . . For starters, using the mod chips requires disassembling the Xbox case and affixing the chip to the circuit board, a task that can require more than 20 soldering connections." David Becker, *Xbox Hacking Not For Amateurs*, CNET NEWS.COM, May 29, 2002, http://news.com.com/2100-1040-924666.html.

[28] "A group of Xbox hackers called 'Free-X' claim to have broken all security measures on the games console without any hardware modifications whatsoever, prompting Microsoft to threaten a legal attack against its members." Patrick Gray, *Hackers Release Xbox Tool Despite Microsoft Threats*, ZDNET AUSTRALIA, July 4, 2003, http://news.zdnet.co.uk/software/0,1000000121,2137053,00.htm?r=1.

[29] *See* Aleph One, *Smashing The Stack For Fun and Profit*, 7 PHRACK 49, http://www.phrack.org/archives/49/P49-14.

operating system, which would enable users to legitimately run Linux on the Xbox without having to evade the DRM system or else the developers would release a working implementation of the evasion system to the Internet.[30]

¶21 Microsoft refused and so the developers made good on their threat. Other developers took advantage of this information, and thus a number of development communities sprung up around the Xbox.[31] This included the Xbox Media Center, an open-source media player capable of playing videos, multi-region DVDs, streaming video and radio from the Internet, and podcasts.[32] Those wishing to play copied games, both fair use backups and illegal copies, also benefited.[33] In many ways, the software pirates were able to free-ride on the efforts of the Linux hobbyists, although Microsoft attempted to portray them in the media as one and the same.[34]

G. i-Opener

¶22 The i-Opener was an Internet appliance,[35] a locked-down Intel Pentium PC designed for web browsing and email, that was released to the US market in November of 1999.[36] The device had limited storage, did not have a hard disk, and stored everything in internal memory. Shortly after launching, the company dropped the price of their device to $99,[37] although reports indicated that the cost to NetPliance (now Tippingpoint, a division of 3Com) for each unit was $400.[38]

---

[30] "Free-X had been trying to negotiate with Microsoft, and was requesting the release of a 'signed' Linux boot loader, which would allow Xbox owners to run the open-source operating system without any hardware modifications or the exploitation of the console. Microsoft would not negotiate, group members have told ZDNet Australia. Group representatives reject claims they are encouraging piracy and accuse the software company of failing to protect its game developers' intellectual property. A signed boot loader won't allow the console to run pirated games, whereas the exploit they have developed will. Free-X say piracy is not something they wish to encourage." Gray, *supra* note 28.

[31] *See generally* The Xbox Linux Project, http://www.xbox-linux.org/wiki/Main_Page (last visited Oct. 26, 2007); Emulators for Xbox, http://worldofstuart.excellentcontent.com/xemus/xbox/xemus.htm (last visited Oct. 26, 2007).

[32] *See generally* The Xbox Media Center Project, http://www.xboxmediacenter.com (last visited Oct. 26, 2007).

[33] *See generally* Hsdemonz, *The Complete Guide to Producing, Extracting, and Burning XBOX ISO Image Files v0.07*, Nov. 21, 2002, http://www.xbox-scene.com/articles/iso-backup-guide.php.

[34] "'We do need to inform you[] . . . that Microsoft Xbox takes pirating of videogames very seriously,' a Microsoft spokeswoman told ZDNet Australia by email. 'The protection of our intellectual properties and copyrights, and those of our partners, is a top priority and therefore we reserve the right to pursue and take action against anyone facilitating piracy of videogames.'" Gray, *supra* note 28.

[35] "Web appliances are cheap, easy-to-use terminals that offer Net access with the flick of a switch. Designed to lure the technologically inexperienced online, they embody much of the promise and risk of the Net Economy." Dominic Gates, *It Slices, Dices, Blends - and Surfs*, COMPUTERWORLD, Sept. 1, 2000, http://www.computerworld.com.au/index.php/id;1099099935.

[36] "In November 1999 we launched our i-Opener service, an all-in-one Internet experience integrating an Internet appliance, access, and consumer portal. Our approach avoids the technological complexities generally associated with using personal computers, or PCs, and traditional Web browsers to access the Internet. We believe our solution provides a simple, seamless and relevant experience that appeals to both new and existing Internet users." SEC Form S-1/A (filed by Netpliance Inc. on Jan. 14, 2000), *available at* http://www.sec.gov/Archives/edgar/data/1097297/0000950109-00-000142.txt.

[37] "The i-Opener was first announced in July 1999. The company set the appliance's retail price at $399 with monthly access fees ranging from $4.95 to $24.95 depending on the number of family members accessing email and customized content . . . . By the time the i-opener hit the market in November, Netpliance had cut the sticker price in half and flattened the access packages to a flat $21.95 . . . . [O]n March 1, they decreased the retail price once more, this time announcing a 50% off sale that would price

¶23 The i-Opener, out of the box, was useless, unless a user subscribed to the dial-up internet service that NetPliance also provided for $22 per month. The device was locked so that it could not connect to any other Internet service provider.[39] NetPliance's own IPO registration statement summed up their business model:

> We currently price our i-Opener Internet appliance below our cost and expect to continue to subsidize the purchase price of our appliance for the foreseeable future. At current pricing levels, a new customer must pay monthly fees for our service for a significant period of time before we recover the purchase price subsidy on that customer's appliance . . . . If we are unable to achieve sufficient revenues from user fees and other sources to cover the subsidies of appliance purchases, we may never become profitable and our business model could fail.[40]

¶24 In February 2000, Ken Segler, a slot-machine designer from Las Vegas and an avid technology hobbyist, posted instructions on his website detailing the process for making a cable that could connect an off the shelf hard disk to the i-Opener and install the Linux operating system onto the device.[41] In addition to the instructions, he also offered to sell the cables himself. Within a week, over 100,000 people had visited his website[42] after news of his hack was posted to the front page of "Slashdot.org," a major technology news website.[43] Within a short period of time, Circuit City stores, the primary retailer of the device, had sold out of the item.[44] Segler himself sold over 200 cables, at $35 each within four days of posting the instructions online.[45]

---

the unit at $99, just one quarter of their originally planned price. At this stage, analysts agreed that the company was losing hundreds of dollars per unit." Kalin R. Harvey, *The i-opener and Open Source*, FRESHMEAT, Apr. 8, 2000, http://freshmeat.net/articles/view/154/.

[38] Posting of John Rohner, former Netpliance engineer, to freshmeat.net: Editorials — The i-Opener and Open Source, http://freshmeat.net/articles/view/154/ (Apr. 10, 2000, 14:53:54), "In March of 1999 I joined the forming company now called Netpliance as their one and only Hardware and Firmware design engineer. The I Opener [sic] is the product of my design efforts . . . . The price of each i-Opener from their Taiwanese manufacturer is $403."

[39] "[O]ur i-Opener Internet appliance comes prepackaged with Internet access delivered over a nationwide dial-up network." Netpliance Inc. SEC Form S-1/A, *supra* note 36. "The i-Opener will not work with other Internet service providers, however, making a subscription effectively mandatory." Ian Fried, *Netpliance Quadruples Price of i-Opener Internet Device*, CNET NEWS.COM, July 5 2000, http://news.com.com/Netpliance+quadruples+price+of+i-Opener+Internet+device/2100-1040_3-242786.html.

[40] Netpliance Inc. SEC Form S-1/A, *supra* note 36.

[41] "In mid-February, Las Vegas electronics engineer Ken Segler walked into his local Circuit City store, ordered a computer — and unwittingly kicked off a small phenomenon. When his order arrived, he tweaked a simple connector cable and turned what was meant to be a closed Internet access 'appliance' — the $99 Netpliance i-opener — into a fully functional, Pentium I-class PC. He published news of his discovery online and soon others were replicating his work." *An I-Opening Hack: $200 PC*, WIRED, Mar. 16, 2000, http://www.wired.com/science/discoveries/news/2000/03/34977.

[42] "Segler has received about 400 emails from system administrators and attorneys — one from a Cornell University professor — inquiring about the cable and his work tweaking the computer. His information page has been hit 100,000 times since Saturday." *Id.*

[43] Posting of Hemos to http://slashdot.org/linux/00/03/11/1216231.shtml (Mar. 11, 2000).

[44] "Within days of Ken's site being featured on the [Slashdot.org] site, pockets of Circuit City stores around the country began to sell out of i-Openers (reportedly the first areas to sell out were in cities that had large research universities nearby)." Harvey, *supra* note 37.

[45] "Four days later, Segler had taken orders for 200 of his modified cables he'd offered for sale at $35 a piece. The cables' connectors are modified to allow the connection of a basic hard disk to the i-Opener, which can then be booted using the user's operating system of choice — Windows, Linux, even the BeOS."

¶25 Rapidly, forums and online communities popped up where users exchanged information on modifying the devices and upgrading them.[46] Users added ethernet network cards, transforming i-Openers into network terminals.[47] Others turned them into car mp3 players and mobile computers.[48] All of these modified devices, for the most part, would not connect to the Netpliance dial-up network, and thus, there would be no subscriber fees to enable the company to recoup its subsidization costs. The devices were sold without any "terms of service" or contract requiring customers to sign up for the internet access service. Customers could walk into Circuit City, pay $100 in cash, and walk out with a device without Netpliance ever learning who had purchased one of their products.

¶26 Within a month, Netpliance revised its business model and instituted a "terms of service" agreement and contract. Customers purchasing the device online from the company's website had to agree to a number of terms. These included:

> By purchasing the i-Opener you are agreeing to use the i-Opener Internet service. The fee is $21.95 a month and will be billed approximately 2 days after the i-Opener is shipped to you. If you decide to deactivate your account within 90 days of receipt, a deactivation fee of $499 will be billed to your credit card.[49]

Netpliance reserved the right to charge customers a termination fee of $499 if the customer violated the "terms of service" agreement. In particular, these terms barred customers from "dissembling, reverse engineering, modifying, adapt or otherwise alter the device."[50] Furthermore, "unauthorized dissemination of trade secrets" was also against the terms, which would probably include telling others how to hack the device.[51]

¶27 Netpliance presumably hoped that the contract would do something to stem the more egregious abuses of their business model. Some customers had reportedly been purchasing nine devices at a time.[52] As Netpliance only required that customers purchase three months of internet service, the company would still only make an additional $65 minus whatever costs were associated with providing Internet access. It certainly did not begin to recoup the $300 that the company was reportedly subsidizing for each device. In July of 2000, Netpliance again changed its business model and began selling the device for $399.[53] By November of 2000, the company laid off over a third of its work-force,[54]

WIRED, *supra* note 41.

[46] *See* i-Opener Running OS's, http://www.linux-hacker.net/imod/imod.html (last visited Oct. 26, 2007); *see generally* i-Opener Info Index, Apr. 2, 2000, http://www.evernex.com/iopener/ (last visited Oct. 26, 2007).

[47] *See generally* i-Opener as a Thin Client, http://ltsp.sourceforge.net/documentation/iopener.php (last visited Oct. 26, 2007).

[48] *See generally* Mouning [sic] My i-Opener in My Truck!, http://home.socal.rr.com/joekewl/io/truckstuff.html (last visited Oct. 26, 2007).

[49] Fred Maxwell, *Expanding the Netpliance i-Opener*, Feb. 8, 2004, http://www.geocities.com/iopener_hack/.

[50] *Id.*

[51] *Id.*

[52] "The result was something of a mini nationwide run on the computer, with some customers buying nine of [sic] i-Openers at a time." *Netpliance Zaps Cheap PC Buzz*, WIRED, Mar. 23, 2000, http://www.wired.com/techbiz/media/news/2000/03/35156.

[53] *See generally* Fried, *supra* note 39.

[54] "Austin's Netpliance Inc. says it will lay off 76 workers, or 54 percent of its work force, to reduce

and by January 2001, the company ceased selling the i-Opener device after its shares had sunk below the $1 level, and risked being de-listed from NASDAQ.[55]

¶28 While some hackers were motivated by the price because, while at $99, the i-Opener was the cheapest Linux platform on the market, others were motivated by the "hack factor" as well as the elegance of the device. It was compact, well-designed, and with a bit of tinkering, was perfect for mobile and in-car use. Several hackers mentioned that they would be happy to pay full price for the devices, but that this was not an option.[56] Netpliance never gave consumers a choice by offering to sell the device at a profit without the required Internet service.

H. Sony Aibo

¶29 The AIBO (Artificial Intelligence Robot) was a product line of several robotic pets designed and sold by Sony. They were first introduced by Sony in 1999 and then later discontinued in 2006.[57] The robots were able to "see" their environment with a built-in camera, recognize verbal commands, express emotion as well as learn and mature based on experiences. Each AIBO had a unique personality shaped by the interactions with their owners. Sony sold over 100,000 of the devices, priced between $850 to $1,500 each.[58]

¶30 In addition to selling the robots, Sony sold add-on software that enabled the robots to assume different personality types as well as perform tricks. Software was loaded onto the robot via a proprietary memory stick which Sony also sold.[59] An enthusiastic community sprang up around the AIBO, and as early adopters are often those most technically skilled, people began to tinker with the software. One particular individual, who was only ever known by his online handle "AiboPet," reached a level of extreme skill in AIBO hacking.[60]

¶31 AiboPet reverse engineered Sony's software and hardware, and soon produced a software package that enabled AIBO owners to teach their pets to dance, speak, obey

---

annual expenses by $6 million. In November, Netpliance cut about 90 employees." *Netpliance to Lay Off 76; President Quits*, AUSTIN BUS. J., Feb. 2, 2001, *available at* http://austin.bizjournals.com/austin/stories/2001/01/29/daily27.html.

[55] *See generally* Maxwell, *supra* note 49.

[56] "A large number of these people publicly stated that they would have been more than willing to have [paid] $300 for the same hardware with a basic modification kit. They didn't want to rip Netpliance off; they just really liked the design of the device and the potential it had. An inexpensive Linux terminal, it turns out, represents quite an untapped market." Harvey, *supra* note 37.

[57] "As part of its ongoing cost-cutting and reorganization effort, Sony has cut its line of robotic Aibo dogs. According to a company representative, more than 150,000 Aibos have been sold since they went on the market in 1999." John Borland, *Sony Puts Aibo to Sleep*, CNET NEWS.COM, Jan. 26, 2006, http://news.com.com/Sony+puts+Aibo+to+sleep/2100-1041_3-6031649.html.

[58] "Aibos, the first mass-produced entertainment robot, have grown in popularity in the three years since they were introduced, with more than 100,000 of the creatures — which cost from $850 to $1,500 — sold worldwide." Eric A. Taub, *Silicon Pets, But the Pride Is Real*, N.Y. TIMES, May 2, 2002, *available at* http://www.nytimes.com/2002/05/02/technology/circuits/02AIBO.html.

[59] "Programming embedded in removable memory chips instructs Aibo how to respond to voices, sounds or visual stimuli and, depending on which program is used, simulate the maturation process." *Id.*

[60] *See generally* David Labrador, *Teaching Robot Dogs New Tricks*, SCIENTIFIC AM., Jan. 21, 2001, *available at* http://www.sciam.com/explore_directory.cfm (select year 2002; then select third page of search results).

wireless commands, and even share the video used for the robot's vision.[61] While AiboPet had reverse engineered the copy-protection scheme used to lock down Sony's propriety memory cards, he did not release this information. The software that he released required a legitimate Sony memory card for each trick that the user wished to install. AiboPet's software stimulated demand for Sony memory sticks, as many fans claimed.[62] AiboPet released his software for free and earned no money from his efforts.

¶32 In October of 2002, Sony lawyers notified AiboPet that he was violating the Digital Millennium Copyright Act (DMCA) and demanded that he remove all software from his website that was based on Sony's proprietary code.[63] The author pulled his code, but spread the word of Sony's actions online. Soon a mass protest by thousands of Aibo owners took place, until, finally, Sony backed down.[64] Within a matter of months, Sony and AiboPet worked out a deal that enabled him to put most of his programs back online. As part of the terms of their deal, AiboPet permitted Sony to adopt and sell any of his ideas and code, should the company wish to do so, royalty-free.[65] While there is no information to suggest that Sony lost money on sales of Aibo, it certainly intended for people to purchase one or more of the many add-on software packages for the robot — which were priced at up to $150 each.

¶33 While the AiboPet episode ended in favor of consumers, for the most part, it does at least demonstrate the fact that consumers often have different intentions for a product than the company that makes them. In this case, Sony was profiting from the initial sale of the robot, so it did not lose any money through the tinkering by users. Sony also sold software for the Aibo and a good argument could be made for the fact that the software that Sony sold and that made by the community were compliments, not substitutes. By and large, people created software to satisfy needs that Sony itself had ignored. Furthermore, the software could only be installed by using a Sony manufactured memory stick, thus meaning that Sony profited even when it did not own the software. This incident was never a case about piracy, merely Sony's desire to retain full control over its platform.

I. Prepaid Phones

¶34 In August of 2006, three Arab-American men were arrested in Michigan with over 1000 prepaid mobile phones, most of which had been purchased at Wal-Mart stores

---

[61] "AiboPet violated that copyright when he cracked the robot's source code to reverse-engineer software that allows Aibo owners to teach their pets to dance, speak, obey wireless commands and share the color video that serves as their vision, among other things. None of the programs are usable without Sony hardware and software. They earned AiboPet no money. He never revealed the encryption code or the program he used to defeat it." *Id.*

[62] "If it had not been for AiboPet's information, his invaluable knowledge and his generosity in sharing it with the Aibo community, I would not have purchased an Aibo, all the various software, [memory] sticks and yes, even my computer, a Sony VAIO, which I only purchased because of its stick reader." *Id.*

[63] "[Y]our site still contains information providing the means to circumvent AIBO-ware's copy protection protocol constituting a violation of the anti-circumvention provisions of the Digital Millennium Copyright Act." Letter from Victor Matsuda, Vice President, Entertainment Robot America, Sony Electronics, Inc. to Aibopet (Oct. 24, 2001) (on file with author), *available at* http://www.cs.cmu.edu/~dst/DMCA/AiboHack/letter2.htm.

[64] Farhad Manjoo, *Aibo Owners Biting Mad at Sony*, WIRED NEWS, Nov. 2, 2001, http://www.wired.com/techbiz/media/news/2001/11/48088.

[65] *See generally* Labrador, *supra* note 60.

around the state.[66] Local prosecutors initially charged them with collecting or providing materials for terrorist acts, although, these charges were later dropped.[67] Federal prosecutors then took an interest in the case and accused the men of defrauding companies TracFone Wireless Inc. and Nokia Corp. by buying the prepaid phones and removing TracFone's proprietary software, making it possible to use the handsets with any cellular provider. A federal judge eventually threw out all of the charges.[68]

¶35 Prepaid mobile phone carriers are a recent arrival to the mobile phone business. They target low income customers who may not have a good credit history or for whom a monthly bill is not practical. Customers purchase a phone from the carrier and then buy "refill cards" which enable them to use additional minutes of service. Prepaid mobile phone carriers sell subsidized handsets that are locked to their network.[69] The phones, often popular models by brands such as Nokia and Sony Erikson, are identical at the hardware level to models used on other networks but contain specific software that prevents them from being used with other mobile phone carriers' networks. The phones are typically purchased in bulk for between $80 to $100 by the prepaid carriers, who install custom software on them, and then resell them to customers for between $20 to $70. The service providers hope to make back their investment by charging a significant markup for the telephone service.[70]

¶36 The three men from Michigan were engaged in a modified form of arbitrage: they bought heavily subsidized devices, removed the software, and resold them to consumers wishing to use them on other networks. Tracfone, the company whose telephones the men had purchased, claims that it has lost millions of dollars because of the practice.[71]

J. Why Phones Are Different

¶37 The typical threat faced by durable good manufacturers is that parasitic competitors will reverse engineer their products, create a compatible add-on service, and then siphon off customers. Through this process, such competitors can free-ride on the subsidy that the manufacturer has placed in each durable good, and thus out-compete on the add-on service, since they do not have any investment that they need to recoup. The prepaid phone business is different, primarily due to the segmentation and structure of the mobile

---

[66] Jason Trahan, *Family, Friends Deny Terror Ties: 3 Accused of Buying Up Cellphones, Targeting Michigan Bridge*, DALLAS MORNING NEWS, Aug. 13, 2006, at 1B, *available at* http://www.dallasnews.com/sharedcontent/dws/dn/latestnews/stories/081306dnmetterrorcharges.19bb76b.html.

[67] *Michigan Prosecutor Dropping Terror Case*, USA TODAY, Aug. 16, 2006, *available at* http://www.usatoday.com/news/nation/2006-08-16-cellphones-terror-charges_x.htm.

[68] "A federal judge threw out conspiracy and money laundering charges Tuesday against three Texas men who originally were accused of planning terrorism, saying there wasn't enough evidence to bring them to trial." *Judge Throws Out Cell-Phone Case*, WIRED, Sept. 5, 2006, http://www.wired.com/science/discoveries/news/2006/09/71726.

[69] "[M]any cellular companies set software locks to control access to their phones, often preventing users from taking that device and using it on a competitor's network." Phuong Cat Le, *Victory for Cell Phone Users: Ruling Allows Them to Break 'Lock' and Switch Carriers*, SEATTLE POST-INTELLIGENCER, Nov. 28, 2006, at B1, *available at* http://seattlepi.nwsource.com/local/293875_unlock28.html.

[70] "[P]repaid phones cost the companies that make them around $80 to $100. They then sell the phones for less — $20 to $70 — in hopes that customers will continue to load more minutes onto the phone, making the company money." Jamie Stengle, *Bulk Cell-Phone Buys Likely for Resale, Not Terror*, ARIZ. DAILY STAR, Aug. 17, 2006, http://www.azstarnet.com/news/142484.

[71] *Id.*

phone market: one set of firms produce the handsets, and another completely different set of firms provide the wireless service. Thus, the wireless service firms all purchase fairly generic inter-operable mobile phone handsets and then attempt to proprietize them through the addition of software locks. Customers who are able to remove this software can, of course, revert these phones back to their previously compatible-with-all-networks status.

¶38 At the hardware level, a phone sold by one wireless company will operate on any other wireless network that uses the same underlying network technology. All of the mobile phone network companies subsidize their telephones, but unlike the prepaid market, the more traditional phone model requires that customers typically sign a contract for phone service. Customers who leave before their contract is up are required to pay a termination fee. Thus, the carriers can be assured that they will recoup the phone subsidization costs, either through the monthly fees charged to customers or through a significant termination fee. Prepaid customers do not sign a contract, and therefore the prepaid operators take on a significant risk. Customers can purchase a phone, with no intention to purchase telephone service and keep the companies from recouping their costs. Some prepaid providers reacted to this by sending DMCA cease-and-desist letters to companies that sold phone unlocking software.[72]

¶39 In November 2006, the Librarian of Congress settled the issue by creating a new exemption to the anti-circumvention provisions of the DMCA. The new rule explicitly permits customers to circumvent the technological protection measures in their mobile phones in order to switch carriers and use the phone on a different network. This was primarily due to petitions from business travelers who wished to use their phones when traveling abroad, and from non-profit groups concerned that useful phones were ending up in landfills.[73]

III. THE RAZOR BLADES

A. Lewis Galoob Toys, Inc. v. Nintendo of America, Inc.

¶40 Nintendo of America ("Nintendo") is a manufacturer of console video game systems including the Nintendo Entertainment System (NES). It has produced games for those devices and sold licenses to other companies enabling them to produce games that would play on Nintendo's hardware. Each Nintendo game cartridge contained two read-only memory (ROM) microchips: a character ROM containing audio-visual information and a game ROM containing the rules and methods of play. Lewis Galoob Toys manufactured a "Game Genie" device, that would enable consumers, through the use of "programming codes" to modify otherwise-unmodifiable parameters in their favorite games. Such modifiable features included accessing levels, bonus features, extra lives, etc. The Game Genie did this by intercepting the communication stream between Nintendo's game cartridges and the NES console. The Game Genie allowed direct,

[72] *See generally* Jennifer Granick, *Free the Cell Phone!*, WIRED NEWS, Sept. 28, 2005, http://www.wired.com/politics/law/commentary/circuitcourt/2005/09/68989.

[73] *See generally* Jennifer Granick, *Cell Phones Freed! Poor Suffer?*, WIRED NEWS, Dec. 6, 2006, http://www.wired.com/politics/law/commentary/circuitcourt/2006/12/72241.

untampered access to the game's character ROM, but would intercept and modify on-the-fly the communication stream between the game console and the game's data ROM.[74]

¶41 Nintendo filed a suit in which it accused Lewis Galoob Toys of contributory copyright infringement. Nintendo claimed that Lewis Galoob Toys sold consumers the Game Genie knowing that consumers would use the device to alter the copyrighted audiovisual sequences in Nintendo's games and as a consequence, create unauthorized derivative works. The district court compared the Game Genie to children modifying the rules to a copyrighted board game, a use which Nintendo admitted would not infringe on a game designer's copyright. The District Court noted that:

> [b]ecause of the technology involved, owners of videogames are less able to experiment with or change the method of play, absent an electronic accessory such as the Game Genie. This should not mean that holders of copyrighted video games are entitled to broader protections or monopoly rights than holders of other types of copyrighted games . . . . Having paid Nintendo a fair return, the consumer may experiment with the product and create new variations of play, for personal enjoyment, without creating a derivative work.[75]

¶42 Nintendo was unable to provide any proof that the Game Genie had diminished or displaced the sales of legitimate games. Customers were not choosing to purchase the Game Genie in lieu of Nintendo's games, as the Game Genie, by itself, was non-functional. The Game Genie needed a game console and a legitimate game to function. Furthermore, Nintendo was unable to provide any proof that it had plans to market games with modifications similar to those that the Game Genie provided. As such, Nintendo was unable to successfully claim that the Game Genie interfered with its own opportunities to sell altered games. Finally, as the Game Genie only modified bits in the communication stream between the game console and the game ROM, there was no derivative work created. After using a Game Genie, a user's game cartridge would have the same data contained within it as when it was purchased from Nintendo, as the Game Genie did not make any permanent changes, nor did it write any data to the game cartridge itself. While the game code being executed by the game console was slightly different than the code supplied by Nintendo, this would disappear once the game was powered off. Without a fixation, there could be no successful claim of a derivative work. The circuit court therefore reversed the district court's grant of a preliminary injunction against Lewis Galoob Toys.[76]

B. Sega v. Accolade

¶43 Sega Enterprises, Ltd. ("Sega") manufactured the Sega Genesis Video Game System as well as producing a number of the games that ran on the system. Sega offered licenses to other companies, which would permit them to produce games for the Sega platform. As part of the license requirement terms, Sega required that game producers exclusively create and release games for the Sega platform, and no competing game system. The Genesis game platform enforced Sega's licensing scheme by refusing to

[74] *See generally* Nintendo of Am., Inc. v. Lewis Galoob Toys, Inc., 16 F.3d 1032 (9th Cir. 1994).
[75] Lewis Galoob Toys, Inc. v. Nintendo of Am., Inc., 780 F. Supp. 1283, 1291 (N.D. Cal. 1991).
[76] *Id.*

execute games which did not contain a specific section of computer code. Sega provided this code sequence to all of its licensees. Accolade, Inc. ("Accolade") produced games for a number of game systems, including other platforms — not including the Genesis — of Sega's. It did not license the rights to produce games for Sega's Genesis platform, and instead its staff reverse engineered a number of Sega games to determine the methods required to interface a game with the Genesis platform.[77]

¶44 Sega sued Accolade because Accolade made a limited number of copies of Sega games during the process of reverse engineering them. Furthermore, Accolade included a short sequence of Sega's code, in order to emulate a licensed game, and trick the Genesis console into executing unlicensed games. The Ninth Circuit disagreed, and noted that Accolade's reverse engineering "led to an increase in the number of independently designed video game programs offered for use with the Genesis console. It is precisely this growth in creative expression . . . that the Copyright Act was intended to promote."[78]

¶45 The Court further confirmed Accolade's right to reverse engineer for the purpose of inter-operability by writing, "If disassembly of copyrighted object code is per se an unfair use, the owner of the copyright gains a de facto monopoly over the functional aspects of his work — aspects that were expressly denied copyright protection by Congress."[79] In order to gain a lawful monopoly over the functional principles underlying a work "the creator of the work must satisfy the more stringent standards imposed by the patent laws."[80]

C. Lexmark

¶46 Lexmark International Inc, ("Lexmark"), a major printer manufacturer, introduced a new line of printers in 2001 which included DRM technology. Each Lexmark made printer cartridge contained a microchip that would malfunction when refurbished by a third party. Lexmark's printers were engineered to detect the presence of a microchip and would reject any cartridge that lacked the microchip, or which had been refilled by a third party. Neither the printer nor the cartridge, both of which contained computer code copyrighted by Lexmark, would function until they had performed a mutual authentication process.[81]

¶47 Lexmark did not adopt this business model for every consumer printer it sold. This was restricted solely to a "prebate" program, in which it would provide consumers with up to a $50 saving over the purchase price of printer cartridges. Such prebate cartridges were sold in boxes that contained a "shrinkwrap" license agreement which required the consumer to use the cartridge only once, and to return it to Lexmark when it was used.[82]

---

[77] *See generally* Sega Enter. Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992).

[78] *Id*. at 1523.

[79] *Id.* at 1536.

[80] *Id*.

[81] *See generally* Lexmark Int'l, Inc. v. Static Control Components, Inc., 387 F.3d 522 (6th Cir. 2004).

[82] Lexmark's subsidized printer cartridges were sold in a box that contained the following license: "RETURN EMPTY CARTRIDGE TO LEXMARK FOR REMANUFACTURING AND RECYCLING. Please read before opening. Opening this package or using the patented cartridge inside confirms your acceptance of the following license/agreement. This all-new cartridge is sold at a special price subject to a restriction that it may be used only once. Following this initial use, you agree to return the empty cartridge only to Lexmark for remanufacturing and recycling. If you don't accept these terms, return the unopened package to your point of purchase. *A regular price cartridge without these terms is available* (emphasis

While every print cartridge sold by Lexmark included one of their DRM microchips, the Lexmark-only functionality was only enabled in those subsidized prebate cartridges. Thus, consumers had a choice: purchase a printer sold at a profit from Lexmark, and use any cartridges they wish, or purchase a subsidized printer from Lexmark, and agree to purchase cartridges from Lexmark only.

¶48 Static Control Components, Inc. ("SCC") introduced the Smartek chip to market in October 2002. SCC had reverse engineered the authentication process used by Lexmark's hardware, and thus produced an inter-operable microchip that, in the eyes of a Lexmark printer, appeared to function identically as one of Lexmark's own microchips. In order to achieve inter-operability, SCC copied wholesale portions of Lexmark's microchip code into their own product. This, it was claimed, was a necessary inter-operability step due to the fact that the contents of the microchip's code was copied into the printer's memory, and verified by the printer's code. The printers were looking for Lexmark's code, and had they found anything else, they would have rejected the third party microchip and its cartridge. Lexmark raised a DMCA claim because Lexmark believed that SCC's microchips circumvented a technological measure that controlled access to Lexmark's Toner Loading Programs.

¶49 On appeal, the Sixth Circuit Court found that Lexmark's microchip code was not copyrightable, due primarily to its "lock-out" functionality, and even were it to be copyrightable, SCC's use would likely qualify as a fair use. The district court had previously found that "Lexmark's authentication sequence effectively 'controls access' to the Toner Loading Programs and the Printer Engine Program because it controls the consumer's ability to make use of these programs."[83]

¶50 The Circuit Court disagreed and said that any consumer, could, if they had the skill, copy the program from the printer's memory, turn it into source code, and disseminate it to the world. Importantly, the court also found that "[n]o security device . . . protects access to the Printer Engine Program Code and no security device accordingly must be circumvented to obtain access to that program code."[84]

¶51 The DMCA only applies to a technical measure that "controls access to a work protected [by a copyright]."[85] As the court had already found that Lexmark's microchip code was not copyrightable, it concluded that the DMCA would not protect the code. SCC could, therefore, not be held to have violated the DMCA by circumventing a technological measure that controlled access to Lexmark's Toner Loading Program.

D. Chamberlain Group, Inc. v. Skylink Technologies, Inc.

¶52 Chamberlain Group, Inc. ("Chamberlain") manufactures a line of garage door openers which contain an added security device featuring "rolling code" technology. Conventional garage door openers are vulnerable to compromise by would-be criminals. Burglars can passively intercept the code sent by the owner's remote to the opener, copy it, and use it at a later date to break into the home. Chamberlain's "rolling code"

---

added)." Memorandum from Marybeth Peters, Register of Copyrights to James H. Billington, Librarian of Congress 173 n.312 (Oct. 27, 2003), *available at* http://www.copyright.gov/1201/docs/registers-recommendation.pdf.

[83] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 253 F. Supp 2d 943, 968 (E.D. Ky. 2003).

[84] *Id.* at 967.

[85] 17 U.S.C. § 1201(a)(2)(A) (2006).

technology changes the entry code after each use, thus defeating the "replay attack" that other garage door openers were vulnerable to.[86]

¶53 Skylink creates ansells universal remote controls that are compatible with multiple garage door openers, including Chamberlain's system. Skylink's remotes bypass the rolling code feature, and when coupled with Chamberlain's openers, the system instead acted as a conventional garage door opener system, in that the same code was used each time. Thus, the system was again vulnerable to interception and replay.[87]

¶54 Chamberlain sued Skylink under the DMCA, claiming that the rolling code function of their software program served as "a technological measure that effectively controls access to a work."[88] The work in question, they claimed, was an operating function of the computer program that controls the garage door opening functionality. Chamberlain claimed that the DMCA was being violated, as Skylink's remote, they claimed, circumvented those technological protection measures.

¶55 Chamberlain claimed in oral argument that "the DMCA overrode all pre-existing consumer expectations about the legitimate uses of products containing copyrighted" and that "pre-DMCA history in the [garage door opener] industry," including the accepted use of replacement universal remotes by consumers, is "irrelevant" as "all . . . uses of products [that circumvent] a technological measure [that] controlled access are now per se illegal under the DMCA unless the manufacturer provide[s] consumers with explicit authorization."[89] On appeal, the Federal Circuit Court disagreed, ruling that "the DMCA did not 'fundamentally alter' the legal landscape governing the reasonable expectations of consumers or competitors."[90] It stated that "[t]he DMCA does not create a new property right for copyright owners. Nor, for that matter, does it divest the public of the property rights that the Copyright Act has long granted to the public."[91] Furthermore, "[a] copyright owner seeking to impose liability on an accused trafficker must demonstrate that the trafficker's device enables either copyright infringement or a prohibited circumvention."[92]

¶56 Skylink was never alleged to have copied or infringed on Chamberlain's copyrighted works (the computer code contained within the garage door opener system). Skylink's circumvention of the rolling code feature was not in order to make an infringing copy of that code but in order to inter-operate with it. In finding for Skylink, the Federal Circuit Court further cemented the right to circumvent in order to build compatible replacement aftermarket products.

E. Vivendi Universal v. Jung

¶57 Davidson & Associates, Inc. doing business as Blizzard Entertainment ("Blizzard") creates, markets, and sells several popular computer games including "StarCraft," "StarCraft: Brood War," and "WarCraft II: Battle.net Edition." Blizzard provides a 24

---

[86] *See* Paul Syverson, *A Taxonomy of Replay Attacks*, *in* PROCEEDINGS OF THE 1994 IEEE COMPUTER SECURITY FOUNDATIONS WORKSHOP VII 187-191 (IEEE Computer Society Press 1994).

[87] *See generally* Chamberlain Group, Inc. v. Skylink Tech., Inc., 381 F.3d 1178 (Fed. Cir. 2004).

[88] 17 U.S.C. § 1201.

[89] C*hamberlain*, 381 F.3d at 1193.

[90] *Id.* at 1194.

[91] *Id.* at 1204.

[92] *Id.*

hour online gaming service, Battle.net, for customers who purchased legitimate copies of its games. The Battle.net service enabled the more than 12 million active users and 200,000 average concurrent users to play against each other over the Internet, instead of competing against computer-controlled enemies, as is normally done in a single-player game. While the online service was provided for free, Blizzard required that a customer have a valid copy of one of its computer games by shipping a license key with each copy of the game. The same license key could not be used multiple times concurrently on Battle.net.

¶58 While the Battle.net service was free, it was not perfect, and in some ways, this stemmed from its huge popularity. Frequent crashes, slow response times and a proliferation of hacks and cheats were the most common complaints.[93] A group of independent programmers founded the "bnetd" project, an alternative to Battle.net, which they hoped would be free of the problems that had plagued Battle.net. It was released as open source software, and was given away for free. The developers of bnetd had no profit motive, and did not gain financially through the bnetd project.

¶59 The developers of bnetd did not have access to the database of compact disc (CD) keys associated with legitimately purchased copies of Blizzard's games. Thus, while they did check for the presence of a CD key, they were unable to verify if a given key was valid or not. They did not institute a check to see if the same key was being used by multiple people at the same time. However, given the open-source development methodology of bnetd and the fact that other people could set up game servers using the freely distributed source code, creating a database of currently valid CD keys would have been difficult, not to mention easy to evade.

¶60 Furthermore, due to the fact that the only authentication measure to connect to Blizzard's official Battle.net server was a CD key, it meant that anyone operating a bnetd server could themselves learn the CD keys of each person connecting to his or her server. Thus, by using one's real CD key on a bnetd server, a user reveals the one secret which could then be used to keep them from connecting to the legitimate Battle.net server in the future.

¶61 Blizzard filed suit and alleged that the bnetd developers violated the DMCA. Blizzard claimed that by circumventing Blizzard's CD key authentication "handshake," bnetd's server permitted unauthorized access to the "Battle.net mode" within Blizzard games. Blizzard claimed that bnetd was "circumventing a technological measure that effectively controls access to a work protected [by the DMCA]" and that the bnetd software was thus prohibited as a technology "primarily designed or produced" for circumvention.[94] Blizzard's argument, essentially, was that each game had two portions of computer code: a single player mode and a multi-player, which was, of course, Battle.net mode. By providing an alternate server for users to connect to, the bnetd developers were allowing unauthorized access to the multi-player portion of the game, without the usual CD key check taking place. In addition to running afoul of the DMCA,

[93] "Battle.net's popularity has been one of its great drawbacks. Frequent crashes and slow response times due to a huge crush of players — especially right after the release of a new game — can often make Battle.net an unpleasant experience. The technical problems are exacerbated by social malfunctions: the malicious killing of some gamers by other players and the proliferation of hacks that give some players unfair advantages." Howard Wen, *Battle.net Goes to War*, SALON.COM, Apr. 18, 2002, http://archive.salon.com/tech/feature/2002/04/18/bnetd/.

[94] 17 U.S.C. § 1201(a)(2).

the bnetd developers were also accused of violating the end user license agreement (EULA) that one was required to agree to before installing any of Blizzard's games. These shrinkwrap licenses forbade any kind of reverse engineering.

¶62 The bnetd developers responded by claiming that the Battle.net portion of the code was not copyrightable, that the code underlying that portion of the game was part of the overall game software, and that any user who had purchased the game had full access to that code in order to run it on his or her computer. Bnetd further claimed that they had only circumvented Blizzard's CD key access control technology for the purpose of achieving inter-operability between Blizzard's game software and bnetd's software. The Eighth Circuit disagreed and affirmed the lower court decision that the bnetd developers had circumvented Blizzard's copy protection, violating the DMCA.[95]

¶63 The outcome of the case is particularly interesting, given the non-commercial nature of the project. There was no corporation to find responsible, no ill-gotten profits. As a result of the case Blizzard was able to have the bnetd internet domain name (bnetd.org) transferred, such that all requests to the website would be redirected to Blizzard's own Battle.net website.[96] Although Blizzard won the case, the bnetd source code continued to be distributed freely online, beyond the physical borders of the United States, in countries where anti-circumvention legislation does not exist.[97] A derivative project, or "fork," of the bnetd project's source code was created. This project is hosted and based in Germany and has an active and thriving community of users and developers.[98]

IV. ANALYSIS

¶64 The purpose of this section is to take a realistic look at the issues presented thus far in the paper. First, the issue of customers hacking or modifying subsidized durable goods ("The Razor") will be addressed. The issue of competitors creating compatible aftermarket goods ("The Blade") will then be discussed.

A. The Razor

¶65 The Razor problem primarily stems from companies choosing to place their trust and make a financial investment in customers with whom they have no prior or contractual relationship. Traditional mobile phone service companies subsidize the cost of handsets but then require that their customers sign a contract with a significant termination fee should the customer wish to end their service. Thus, these companies can be sure that they will recoup their investment, either through ongoing subscription fees or a termination fee. In order to further restrict their potential losses, these companies

[95] Davidson & Assocs. v. Jung, 422 F.3d 630, 631 (8th Cir. 2005).

[96] The Internet domain name www.bnetd.org will now take you to Blizzard's own website, http://www.blizzard.net. *See* Battle.net, http://www.bnetd.org (last visited Oct. 25, 2007).

[97] "On 21st February 2002, the bnetd site was shut down at the demand of Blizzard Entertainment as an alleged DMCA violation. (See Blizzard's stance on battle.net emulation.) Since I do not believe that bnetd is proscribed under the DMCA, and since the DMCA is not applicable in the UK, some bnetd files, links, and information are made available here in the hope that development will continue." Owen Dunn, *Bnetd, a Free Battle.net Server*, http://www.chiark.greenend.org.uk/~owend/free/bnetd.html (last visited Oct. 25, 2007).

[98] *See* Player vs. Player Gaming Network, http://www.pvpgn.org/ (last visited Oct. 25, 2007).

require that their customers have a good credit rating, so that the threat of a termination fee or negative credit report will be taken seriously.[99]

¶66 Prepaid phones and gaming consoles are just two of the many subsidized projects that adopt the unknown customer subsidization business model, and due to the fact that they target younger customers, and those with irregular income patterns, the termination fee and contract model will simply not work. The prepaid phone companies take great efforts to advertise that their phones do not require any contract.[100] Since the Librarian of Congress issued a DMCA exception to those who wish to hack their phones, the prepaid phone market has not collapsed. Subsidized phones are still available to customers, but instead, the vendors have adapted. Consumers may now only buy two or three phones per store-visit,[101] and the phone manufacturers have released new phones that are more difficult to unlock. It is, of course, an arms race, as hackers will work to discover new methods of phone unlocking. With a profit of $50 per subsidized handset, they have a strong financial incentive to find a way. Tracfone has also filed suit against the Librarian of Congress to reverse the recently introduced DMCA exception.[102]

¶67 One clear lesson can be learned from the business cases presented earlier in this paper. A common theme that can be seen with both Microsoft's Xbox and Netpliance's i-Opener is that the Linux/open source developers community makes for a considerable adversary. If a single DRM system protects a product against both piracy and open source hackers tinkering with the product, the odds do not bode well for the anti-piracy system's success. This very design flaw was present in both the Xbox as well as the DVD system. Companies should either embrace the Linux community or, at the very least, design a separate DRM system that keeps the Linux hackers at bay.

1. Contract Law

¶68 The Netpliance customers who hacked their i-Opener were violating the shrinkwrap license that they had accepted when they opened the box. Likewise, the Xbox purchasers or the prepaid phone customers would have violated a license, should the vendors have chosen to include one in the packaging. While the companies may have some kind of claim against their customers for violating the contract, for the most part, it is a moot point.

¶69 If a customer is able to purchase the item in cash, in person, without ever establishing a permanent relationship with the company, there is no practical method by which the company can identify the customer and, thus, go after them for violating the terms of the contract. This assumes, of course, that the company has a way of determining that the customer has indeed violated the contract, as it is exceedingly

[99] *See generally* Tim Wu, *Wireless Carterfone*, 1 INT'L J. COMM. 389 (2007).

[100] "T-Mobile prepaid plans give you wireless access with less commitment, so you can pay — and talk — as you go. With no annual contract, no credit check, and no monthly bill, prepaid plans are a simple, direct way to go mobile." Prepaid Calling Plans: T-Mobile To Go Pay As You Go, http://www.t-mobile.com/shop/plans/default.aspx?plancategory=4 (last visited Oct. 25, 2007).

[101] "Wal-Mart Stores Inc. plans to limit each customer to two prepaid cell phones per purchase amid complaints that entrepreneurs are buying the subsidized handsets by the hundreds to resell at a profit, according to people familiar with the matter." Bruce Meyerson, *Wal-Mart Limits Prepaid Cell Phones to 2*, MSNBC.COM, Oct. 20, 2006, http://www.msnbc.msn.com/id/15335329/.

[102] Posting of Fred von Lohmann to Electronic Frontier Foundation Deeplinks Blog, http://www.eff.org/deeplinks/2006/12/tracfone-sues-block-cellphone-unlocking-exemption (Dec. 6, 2006).

difficult to find out what happens to a product once a customer takes it home. There is a big difference between hacking an Xbox and leaving it unopened in the original box. However, from the financial perspective of the manufacturer, both of these situations have the same impact: a wasted subsidy.

2. Who Can You Go After?

¶70 Tracfone claims to have lost millions of dollars through customers who reprogrammed their phones.[103] Netpliance's i-Opener was a commercial flop and large numbers of the purchasers of the product were those who solely wished to hack it. Xbox was a commercial success, although Microsoft clearly lost money on every Linux hacker who bought the console only to then hack it.

¶71 Assuming that the companies are able to compile a list of who their customers are, and which of them have hacked their devices, the next question to be asked is what can the companies then do, and who can they go after?

¶72 *a) Go after the customers.* — Suing individual customers is not a particularly effective strategy, even if they have cost you money. It is a strategy that has been widely used by the Recording Industry Association of America (RIAA) in its campaign against unauthorized copying of music. The campaign has won the RIAA scorn and negative publicity, especially in the more extreme cases when they have gone after a 12-year-old child,[104] a 71-year-old grandfather,[105] and the deceased.[106] Bad publicity aside, it is impossible to sue hundreds of thousands of people, and even if one could, it is unlikely that they, their family, or their friends would ever turn into legitimate customers afterwards.

¶73 *b) Go after those who create the hack.* — Some in academia have recently begun to write about the impact of so called "Superusers."[107] While thousands of independent programmers have worked on the Linux operating system, most DRM circumvention is done by a handful of skilled individual users. Some commentators justify the DMCA's fairly Draconian rules by pointing to the threat that a single skilled programmer can pose to a DRM system, and thus a company's bottom line.

¶74 The computer programmer who reverse engineered the DRM system that protected DVDs was a teenager from Sweden. He was beyond the jurisdictional limits of the US legal system. While the Motion Picture Association of America (MPAA) exerted pressure to have him charged, his case was later thrown out by a Swedish judge.[108]

---

[103] Stengle, *supra* note 70.

[104] Jefferson Graham, *Recording Industry Sues Parents*, USA TODAY, Sept. 15, 2003, at D4, *available at* http://www.usatoday.com/tech/news/techpolicy/2003-09-15-riaa-parents_x.htm.

[105] *Id*.

[106] Posting of Mike Yamamoto to CNET News.com News Blog, http://www.news.com/8301-10784_3-6110271-7.html (Aug. 28, 2006 13:37 PDT).

[107] Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. DAVIS L. REV. (forthcoming 2008), *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=967372.

[108] Nina Berglund, *DVD-Jon Wins New Legal Victory*, AFTENPOSTEN (Nor.), Dec. 22, 2003, *available at* http://www.aftenposten.no/english/local/article696330.ece.

¶75 While it is possible to go after Americans who reverse engineer, it is quite easy for them to anonymously release their information.[109] Aggressive activities by software companies against those in the computer security community have done much to encourage the anonymous release of security vulnerability information. It has not stopped the disclosure of research but forced those security experts to release their work anonymously, and not to work with the companies directly.[110]

¶76 *c) Go after those who share information detailing the hack, and distribute it online.* — Unable to go after the creator of the hack, the MPAA then attempted to shut-down U.S. based website operators who posted copies, or even links to other copies of the code.[111] These individuals did not reverse engineer the DRM system themselves but were merely providing a link so that others could download and then use the code. The court surprised many commentators when it sided with the MPAA, and one of the website operators was forced to remove the links from his site. The DeCSS source code is still widely available on the Internet, both from servers outside the United States,[112] and sites within the US.[113] In particular, a professor at Carnegie Mellon University who provided expert testimony at the CSS trial still has the source code on his official university homepage.[114]

¶77 While the MPAA won its lawsuit, the only long term effect was to incentivize politically aware Internet users to engage in a modern form of civil disobedience by making copies available on their own websites ("mirroring"). This has happened on a number of occasions, including Diebold's electronic voting machine source code,[115] confidential internal documents belonging to Church of Scientology,[116] and the DRM system used by the HD-DVD platform.[117] Even in the highly unlikely case where a copyright holder was able to use the DMCA and other tools to force every webmaster in the world to remove circumvention information, censorship resistant anonymous publishing systems have already been designed and deployed that would further frustrate

---

[109] *See generally* Tor: Anonymity Online, http://tor.eff.org (last visited Oct. 25, 2007).

[110] "In mid-2001 an anonymous programmer discovered a vulnerability in Microsoft's proprietary e-book DRM system, but refused to publish the results, citing DMCA liability concerns." ELECTRONIC FRONTIER FOUNDATION, UNINTENDED CONSEQUENCES: SEVEN YEARS UNDER THE DMCA, at 4 (2006), http://www.eff.org/files/DMCA_unintended_v4.pdf (citing Wade Roush, *Breaking Microsoft's e-Book Code*, TECH. REV. 24 (Nov. 2001)); *see also* Christopher Sasaki, *Anonymous Hacker Shows Xbox 360 Exploit*, PLAYFEED, Jan. 1, 2007, http://games.gearlive.com/index.php/playfeed/article/anonymous-hacker-shows-xbox-360-hack-01010955/.

[111] *See generally* Universal City Studios, Inc. v. Reimerdes, 111 F. Supp 2d 294, 294 (S.D.N.Y. 2000), *aff'd sub nom.* Universal City Studios, Inc. v. Corley, 273 F.3d 429 (2d Cir. 2001).

[112] *See* DeCSS Central, http://www.lemuria.org/DeCSS/ (last visited July 4, 2007); DeCSS: Watch Your DVD's on Your Favorite OS, http://www.free-dvd.org.lu/ (last visited Oct. 25, 2007); DeCSS Software Distribution Center, http://www.pigdog.org/decss/source/decss_mirror.html (last visited Oct. 25, 2007).

[113] Crackmonkey W@R3Z, http://crackmonkey.org/warez.html (last visited Oct. 25, 2007); DeCSS Mirror, http://decss.robinlionheart.com/ (last visited Oct. 25, 2007).

[114] Dave Touretzky, *Gallery of CSS Descramblers*, http://www.cs.cmu.edu/~dst/DeCSS/Gallery/ (last visited Oct. 25, 2007).

[115] Declan McCullagh, *Students Buck DMCA Threat*, CNET NEWS.COM, Nov. 3, 2003, http://news.com.com/Students+buck+DMCA+threat/2100-1028_3-5101623.html.

[116] Operation Clambake, The Inner Secrets of Scientology, http://www.xenu.net/ (last visited Oct. 25, 2007).

[117] Chilling Effects Clearinghouse, AACS Licensor Complains of Posted Key, http://www.chillingeffects.org/notice.cgi?sID=3218 (last visited Oct. 25, 2007).

such a censorship effort.[118] Where there is no profit motive and thus no money trail to follow and where information is being given out for the "hack value" or pleasure of reverse engineering, it will be next to impossible to put the proverbial genie back into the bottle. Cyber-activist John Gilmore accurately described the futility of attempting to force webmasters to take down content when he stated, "The Net interprets censorship as damage and routes around it."[119]

3. Fixing the Problem with Technology

¶78 Technology and, in particular, information security in particular, are always an arms race. Worse, it is an unfair playing field, where the hackers and tinkers are engaged in a form of asymmetric warfare with technology companies. Unfortunately for the manufacturers to be successful, they must defend themselves every single time to protect their business model while the hackers only need to succeed once. The companies have a limited quantity of development man-hours, while an army of open source programmers toil away at breaking the DRM system in their seemingly unlimited spare time. The odds are stacked against those companies trying to design an effective DRM system. It is for this reason that there are very few, if any, DRM success stories.

¶79 Microsoft clearly learned from its Xbox experience, and thus its more recent platform the Xbox 360 shipped with a much stronger DRM system. Predictably, a group of Linux hackers were again able to reverse engineer this system and get Linux booting on the new gaming system.[120] Microsoft did at least learn enough to de-align the various groups. Hobbyists can now play their own "homebrew" games on the Xbox without having to resort to reverse engineering. In permitting this kind of activity, Microsoft has at least removed one group who would otherwise be hard at work attacking their DRM technology.

¶80 In the end, the strategy of selling a subsidized good to a complete stranger may prove to be a very risky one. For those companies that are able to create strong enough protection systems, high profits will await them. For those whose protections are cracked, their bottom line may suffer. To those potential manufacturers thinking of adopting the unknown customer subsidized durable good business model, *caveat venditor*.

B. The Blade

¶81 Based on the post-DMCA case history, the courts seem to have taken the position that the DRM in hardware items cannot be protected through anti-circumvention rules. Examples of this have so far included garage door openers and printers, but could grow to include car parts, cameras, and coffee makers. For those companies manufacturing physical durable goods, they may have to seek other methods of going after those competitors who make compatible goods. One other major printer manufacturer seems to

---

[118] *See generally* Tor, *supra*, note 109; The Free Network Project, http://freenetproject.org/ (last visited Oct. 25, 2007).

[119] Quotations About the Internet, http://cyber.law.harvard.edu/people/reagle/inet-quotations-19990709.html (last visited Oct. 25, 2006).

[120] Josh Evers, *Microsoft Patch Stops Linux on Xbox 360*, NEWS AT CNET.CO.UK, Mar. 6, 2007, http://news.cnet.co.uk/gamesgear/0,39029682,49288221,00.htm.

have recognized the failings of the DMCA to protect this business model, and has instead opted to use patent law to go after aftermarket print cartridge manufacturers.[121]

¶82 While the bnetd decision is just one case, it seems that the courts are taking a completely different view when it comes to software products and their aftermarkets. The software market is more interesting, primarily due to the distribution costs brought about through the information economy. It is very difficult to make replacement printer cartridges for free; however, a group of hobbyist programmers can quite easily create a software product and make it available online for free. This is primarily due to the near-zero cost of distributing goods online.

¶83 The stakes for electronic good manufacturers are now higher than ever before. Blizzard, which previously gave away access to its Blizzard.net service for free, now charges more than eight million active customers $15 per month for access to its World of Warcraft online services.[122]. While the company previously was merely defending its right to control the user experience, any project similar to bnetd for the company's World of Warcraft game would now significantly threaten its revenue stream.

1. Financially Motivated Versus Open Source Competitors in Software Aftermarkets

¶84 In the case of software durable goods, if a company makes a competing aftermarket product, the company producing the primary durable good should be able to use the DMCA to go after its competitor. That, at least, is the precedent that bnetd has set. However, if a compatible aftermarket good has been created and released for free by hobbyists on the Internet, there is very little that the manufacturer can do to shut its new competitors down. As previously explained in the Razor section, the DMCA does not reach beyond the physical borders of the United States. Furthermore, while it can be used against US based programmers, this merely forces them to adopt pseudonyms and release their code anonymously. As is always the case, it is far easier to go after a competitor who has a physical presence, a bank account, and physical assets. Going after open-source programmers is the Internet equivalent of being the weaker side in asymmetric warfare. The stronger opponent, a distributed network of programmers, will dodge and evade any takedown efforts.

2. A Moral Right To Hack?

¶85 While those companies making prepaid phones may not be able to do anything to stop customers from purchasing their phones, resetting the software, and then reselling them, it is worth exploring the question of morality. Simply put: is it "right" to do what these men did, when they bought 1000 phones, wiped their software, and re-sold them? Is it morally right to buy an Xbox, and then turn it into a cheap living room entertainment system? Likewise, is it morally right to buy a subsidized printer and then only purchase third-party cartridges for it? By and large, the morality question is the same for those

[121] Jacqui Cheng, *Epson Wins Preliminary Ruling Against Aftermarket Cartridge Manufacturers*, ARS TECHNICA, Apr. 8, 2007, http://arstechnica.com/news.ars/post/20070408-epson-wins-preliminary-ruling-against-aftermarket-cartridge-manufacturers.html.

[122] Press Release, Blizzard Entm't, World of Warcraft Surpasses 8 Million Subscribers Worldwide (Jan. 11, 2007), *available at* http://www.blizzard.com/press/070111.shtml.

who hack the razor and for those who seek cheaper compatible blades. Is it right to buy a subsidized good and then knowingly stop the company from recouping its investment?

¶86 The two extremes can be seen in the case of the Netpliance i-Opener and the Lexmark prebate printers. Netpliance sold only one kind of i-Opener: one that was subsidized. Thus, any customer that wished to purchase one and put Linux on it had to essentially take money from Netpliance's pocket. Lexmark, on the other hand, sold multiple printers, and only applied a DRM scheme to their subsidized models. Customers who wished to use third-party print cartridges with their printers could buy a full price printer, and customers who were willing to be restricted to Lexmark's own cartridges could purchase the subsidized printer. The problems for Lexmark arose when customers greedily wished to use a subsidized printer with cheap third-party ink.

¶87 It is very easy to sympathize with the Linux hackers who reverse engineered the i-Opener, those who wished to get Linux running on their Xbox, or those who reverse engineered the DVD DRM scheme so that they could play legitimately purchased DVDs on their Linux home computers. In all three of these cases, customers essentially had a binary choice: purchase the system, or don't. If any kind of "right to reverse engineer" or "right to hack" argument can be made, it should apply to these customers.

¶88 However, those who wished to evade the DRM system used by Lexmark are on much shakier moral ground. If a company sells two different models: one subsidized and locked via DRM, and another sold at a modest and reasonable profit, it is very difficult to make a solid argument for a right to hack. The consumer then, after all, has a perfectly reasonable means by which they can purchase an unencumbered product. Those who choose to purchase the subsidized product and then strive to strip out the DRM are then engaged, essentially, in theft. They are not defending a right to hack but are merely unfairly leeching resources from another company. This is clearly wrong.

V. Conclusion

¶89 This paper has explored a number of issues related to risky business models in which companies sell unsubsidized, technology-based consumer goods and then hopefully recover their investment through aftermarket sales. Such companies often end up fighting off competitors wishing to leverage the company's subsidized platform to sell their own compatible aftermarket products. They can also end up fighting their own customers who wish to use the products in creative, but unprofitable ways. For the company producing and subsidizing the items, both situations can lead to the same end result: financial losses for a subsidized good which will not lead to future sales.

¶90 Companies wishing to follow this business model must take care, as it is a potentially profitable, yet extremely dangerous strategy. Selling to customers with whom a company has no prior business relationship, and often has no means of reliably identifying, can be financial suicide. It is simply too easy for parasitic businesses to take advantage of a company's subsidization to make their own businesses profit — be they mobile phone resellers or makers of printer ink cartridges.

¶91 This paper also explored a number of case histories of failed products that utilized Digital Rights Management technology to try and keep tinkering customers at bay. In all of the cases presented, open source programmers were able to out-wit and out-engineer the companies manufacturing locked-down products. The lesson from such cases is clear: if the financial success of a product depends on keeping motivated Linux hackers

from successfully accessing the guts of the device, its manufacturer may want to go back to the drawing board. At the very least, companies should not use the same DRM technology to deny access to both open-source hobbyists wishing to tinker with the device and also software-copying pirates wishing to avoid paying for the company's own high-priced aftermarket items.

¶92 Furthermore, while the law (be it a shrinkwrap contract or the DMCA) may be on the side of the companies producing these goods, in reality, their options for defending themselves and their business models are quite limited. Suing your customers will not accomplish much beyond ruining your reputation, while those advanced users who actually reverse engineer the products and share the information of the hack are often either in another country, or post the information to the Internet anonymously.

¶93 New laws will not help to shore up the subsidized razor and blade business model. Likewise, there will be no unbreakable DRM magic bullet to protect such products from hackers, curious customers, and parasitic competitors. It's a dangerous market — but with the possibility of reaching the large untapped market of customers for whom relationships and credit histories are not an option, many companies may still choose to take the risk. *Caveat venditor*.