Legal Issues Affecting Creation And Implementation Of DRM Systems

Gabriel M. Ramsey, Esq.
Orrick, Herrington & Sutcliffe LLP

I. INTRODUCTION

Since the late 1990s, DRM systems have become increasingly prevalent in the videogame industry. With annual losses in the billions due to videogame piracy, DRM is potentially an important component of the solution. However, the place of DRM in the world of digital content has been highly contested. Thus, concomitantly with the increased attention to DRM in recent years, a substantial body of law has developed out of the conflict around these technologies as well. It is important for those tasked with selecting, implementing or managing DRM systems to understand the implications of the law in this area, in order to ensure the strongest protection and the least legal exposure. Here we explore two different legal topics pertinent to assessing DRM technologies. First, we consider how legal developments concerning the Digital Millennium Copyright Act ("DMCA") affect the level of protection afforded by different types of DRM systems. Second, we address the potential for legal exposure from lawsuits by users claiming damage related to the implementation of DRM technology.

II. SELECTING A STRONG DRM SYSTEM UNDER THE DMCA

A. Background: The DMCA's "Anti-circumvention" Provisions

In 1998, the DMCA was passed, prohibiting circumvention of "technological protection measures" which control copying and access to copyrighted content.[1] In other words, the DMCA acts as a legal mechanism to enforce DRM systems. If a content owner implements DRM technology limiting the use of its content, and someone hacks the system in order to make unauthorized use of the content, that person may be liable under the DMCA. Violators may be ordered to cease their conduct, have their devices impounded, modified or destroyed and may be subject to substantial damages awards (including paying plaintiff's costs and attorneys fees). Repeat offenders may have damages awards increased up to three times. The DMCA also prescribes significant criminal penalties for willful violations undertaken for commercial advantage or private financial gain.

The DMCA contains two different regimes related to "circumvention of technological protection measures." The first regime addresses circumvention of measures that "effectively control access to a work."[2] The second regime addresses circumvention of measures that

[1] As an initial note, it is important to realize that the DMCA only prevents circumvention of measures designed to protect matter protected by copyright. Creative content, source code or even object code constitute such copyrightable material. For example, see *Storage Tech. Corp. v. Custom Hardware Eng'g & Consulting, Inc.*, 421 F.3d 1307, 1318 (Fed. Cir. 2005) (DMCA "prohibits only forms of access that bear a reasonable relationship to the protections that the Copyright Act otherwise affords copyright owners.")

[2] 17 U.S.C. § 1201(a)(1)(A), (a)(2).

"effectively protect a right of a copyright owner"—*i.e.* protects against copying.[3]

The "access control" regime states very broadly that "*no person* shall circumvent a technological measure that effectively controls access to a work"—thus encompassing anyone who simply uses such circumvention technology. The access control regime also prohibits manufacture or distribution of devices primarily designed for circumventing access controls. By contrast, the "copy control" regime *only* prohibits manufacture or distribution of devices primarily designed to circumvent copy protection measures. Those only *using* the devices do not face liability under the copy control framework.

Obviously, then, whether a given DRM system is characterized as an "access control" measure or "copy control" measure substantially affects the level of protection it will be afforded under the DMCA. Being able to pursue the users of circumvention tools, as is possible for access controls, may be particularly powerful where large operations circumvent DRM systems in order to make and sell infringing copies, but do not themselves create or distribute circumvention tools. Since the DMCA was enacted, courts have provided guidance regarding the definition of the "access control" and "copy control" categories. Although there may be many commercial and policy considerations in deciding whether and how to implement DRM, it is clear that if the system is an "access control" measure, broader protection is possible. This attribute can be viewed as a component of the overall strength of the technology.

B. Defining Circumvention Of "Access Control" And "Copy Control" Systems

1. What Is An "Access Control" Measure?

The DMCA states that an access control system is one that "effectively controls access to a work protected under [the Copyright Act]."[4] A measure "effectively controls access to a work" if:

> the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work.[5]

The House legislative report further clarifies that that the access control provision "applies when a person has not obtained authorized access to a copy . . . of a work for which the copyright owner has put in place a technological measure that effectively controls access to his or her work."[6]

Cases interpreting the DMCA reveal that a defining feature of an "access control" measure is that it completely prevents any experience of the copyrighted work without the authorized application of some technology. For example, early in the DMCA's history, one

---

[3] 17 U.S.C. § 1201(b)(1).
[4] 17 U.S.C. § 1201(a)(1)(A).
[5] 17 U.S.C. § 1201(a)(3)(B).
[6] H.R. 105-551

court found that the "CSS" system protecting commercial DVD content was an access control, observing:

> One cannot gain access to a CSS-protected work on a DVD without application of the three keys that are required by the software. One cannot lawfully gain access to the keys except by entering into a license with the DVD CCA under authority granted by the copyright owners or by purchasing a DVD player or drive containing the keys pursuant to such a license. In consequence under the express terms of the statute, CSS 'effectively controls access' to copyrighted DVD movies.[7]

One good online example, in the gaming context, is Blizzard's implementation of an authentication sequence between locally running games and its "Battle.net" server. The authentication regime involved the exchange of CD Key information and random numbers, enabling the server to confirm that the CD Key was valid and not in use by another player. The authentication sequence was required before any user access to the online Battle.net mode and associated content was possible. Defendants created their own emulated version of the Battle.net server, bypassing this authentication regime. This allowed unauthorized access to the Battle.net code and associated game content and further enabled the use of pirated games. Defendants were found to have circumvented an access control measure.[8]

In the console context, there have been a number of cases involving access control measures in the PlayStation and PlayStation 2. Sony's design of its console to play only those games with codes matching the geographical location of the console itself was considered an access control measure. Defendant's product, which caused the console to believe that import games were in fact U.S. games, improperly circumvented this measure.[9] Likewise, in a more recent series of cases, codes contained on authentic PlayStation games enabling the console to distinguish them from pirated copies were considered access control measures. Defendants' products, including "HDLoader" (which enabled unauthorized copies of games to be made on a connected hard drive) and a variety of mod chips allowed users to bypass the authentication system, thus circumventing the access control system.[10] In each of these instances, the technological measures were designed to wholly prevent use of the games, unless authorized by the system.[11]

Encryption is an another important component of an access control measure. For example, the court addressing the Blizzard system observed that the authentication handshake

---

[7] *Universal Studios v. Reimerdes*, 111 F. Supp. 2d 294, 317-318 (S.D.N.Y. 2000)
[8] *Davidson & Assocs. v. Internet Gateway*, 334 F. Supp. 2d 1164, 1169 (E.D. Mo. 2004)
[9] *Sony Computer Entm't Am., Inc. v. GameMasters*, 87 F. Supp. 2d 976, 987-988 (N.D. Cal. 1999).
[10] *Sony Computer Entm't Am., Inc. v. Divineo, Inc.*, 2006 U.S. Dist. LEXIS 74878 (N.D. Cal. 2006); *Sony Computer Entm't Am., Inc. v. Filipiak*, 406 F. Supp. 2d 1068, 1070 (N.D. Cal. 2005)
[11] There are other relevant examples as well. Scrambling of satellite television transmissions was considered an access control measure circumvented by defendant's unauthorized descrambling devices. *Comcast of Ill. X, LLC v. Hightech Elecs., Inc.*, 2004 U.S. Dist. LEXIS 14619 (N.D. Ill. 2004). Likewise, RealNetworks' authentication regime between its RealPlayer and RealServer was considered an access control measure. *RealNetworks, Inc. v. Streambox, Inc.*, 2000 U.S. Dist. LEXIS 1889, 6-7 (W.D. Wash. 2000). In each case, the content could not be played at all unless proper authentication was achieved through the technological measure.

was encrypted. Likewise, the courts dealing with CSS have emphasized that the CSS keys are encrypted and subject to other security measures.[12] The more general issue here is that a measure cannot "effectively" control access if it does not in fact protect the content in some manner. For example, printer manufacturer Lexmark was unsuccessful in arguing that an authentication sequence effectively controlled access to its copyrighted printer engine program because any customer that bought the printer could read the literal code directly from the printer memory, without any authentication sequence.[13]

On the other hand, if the efficacy of the access control measure has been jeopardized by unauthorized conduct of third parties, courts will be unwilling to apply this rationale. For example, in the case of CSS, the CSS keys were alleged to be widely available on the Internet as a result of unauthorized conduct by third parties. Nonetheless, the court still regarded the measure as one which "both effectively controls access to DVDs and effectively protects the right of a copyright holder," as one could not gain authorized access to the keys without entering into a license.[14] Generally, though, the greater the encryption and other steps to secure content, the greater the chance that the DRM system will be considered an "effective" access control measure.

2. What Is A "Copy Control" Measure?

Under the DMCA, a copy control measure is one that "effectively protects a right of a copyright owner [under the Copyright Act]"[15] A DRM system meets the definition if:

> the measure, in the ordinary course of its operation, prevents, restricts, or otherwise limits the exercise of a right of a copyright owner under this title.[16]

The House legislative report specifies that this provision "applies when a person has obtained authorized access to a copy . . . of a work, but the copyright owner has put in place technological measures that effectively protect his or her right under [the Copyright Act] to control or limit further use of the copyrighted work."[17]

Unlike the access control measures, the key feature of DRM systems in this category is that they do not restrict the ability to initially access or execute the game, but they *do* restrict the ability to reproduce, distribute or publicly perform or display the game, or to create "derivative works" from the game.

---

[12] *Universal Studios v. Reimerdes*, 111 F. Supp. 2d 294, 310 (S.D.N.Y. 2000) (noting that CSS was licensed under strict security requirements "to ensure . . . that compliant devices could not be used to copy as well as merely play CSS-protected movies"; CSS licensees "may not . . . make equipment that would supply digital output that could be used in copying protected DVDs.")
[13] *Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 387 F.3d 522, 546-547 (6th Cir. 2004)
[14] *321 Studios v. MGM Studios, Inc.*, 307 F. Supp. 2d 1085, 1095 (N.D. Cal. 2004)
[15] 17 U.S.C. § 1201(b)(1)(A)
[16] 17 U.S.C. § 1201(b)(2)(B)
[17] H.R. 105-551

A good example of a purely "copy control" measure are the restrictions enabled in Adobe's eBook format. When eBooks for the Adobe eBook Reader format are sold, the publisher or distributor can authorize or limit the purchaser's ability to copy, distribute, print, or have the text read audibly by their computer. The eBook Reader is designed to manage such digital rights, so that in the ordinary course of its operation, the Reader effectively permits the publisher or distributor to limit the exercise of rights under the Copyright Act. The defendant sold a product called "Advanced eBook Processor" which allowed users to remove use restrictions from files formatted for the Adobe eBook Reader. The program allowed eBooks to be converted to "naked PDF" format that is readily copyable, printable, and easily distributed electronically. It was argued that this was a circumvention of a copy control measure, as the eBook could be initially read by any purchaser but imposed limits on *subsequent* use. Interestingly, the case was prosecuted under the DMCA's criminal provisions. While the jury ultimately found that the technology violated the DMCA, it acquitted the defendants on the basis that they lacked "willful" intent to violate the DMCA.[18]

Similarly, Macrovision's Analog Copy Protection technology hinders the making of analog videotape copies of DVDs already accessible by a user, but does not in any way prevent initial access to the work. This too was found to be a copy control measure. This is because in the ordinary course of its operation, it prevents, restricts or limits the exercise of the copyright owner's rights—namely by hindering the making of videotape copies of protected DVDs. By contrast, such technology does not, in the ordinary course of its operation, require the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work, and is therefore not an access control measure.[19]

Often, copy control measures have been considered secondary features of access control systems, or intertwined with such systems. For example, one court considering the CSS system found that the limits on initial access to a DVD prevent subsequent copying, observing that while it was "technically correct that CSS controls access to encrypted DVDs, the purpose of this access control is to control copying of those DVDs, since encrypted DVDs cannot be copied unless they are accessed.[20] Likewise, the authentication regime between RealNetworks' local RealPlayer and its proprietary server involved first, a secret handshake, characterized as an access measure, and the content then delivered contained a distinct "copy switch" which was characterized as a copy control measure.[21] Further, the scrambling of satellite television content was also considered a copy control measure, in addition to being an access control measure.[22]

Like access controls, copy controls must "effectively" protect the rights of a copyright owner. In once case, it was found that embedded bits which expressed the copyright owner's

---

[18] *United States v. Elcom Ltd.*, 203 F. Supp. 2d 1111 (N.D. Cal. 2002); http://news.com.com/2100-1023-978176.html

[19] *Macrovision v. Sima Prods. Corp.*, 2006 U.S. Dist. LEXIS 34496 (D.N.Y. 2006)

[20] *321 Studios v. Metro Goldwyn Mayer Studios, Inc.*, 307 F. Supp. 2d 1085, 1095 (N.D. Cal. 2004) ("[i]t is evident to this Court, as it has been to previous courts, that CSS is a technological measure that both effectively controls access to DVDs and effectively protects the right of a copyright holder.")

[21] *RealNetworks, Inc. v. Streambox, Inc.*, 2000 U.S. Dist. LEXIS 1889, 6-7 (D. Wash. 2000)

[22] *Comcast of Ill. X, LLC v. Hightech Elecs., Inc.*, 2004 U.S. Dist. LEXIS 14619 (D. Ill. 2004)

preferences with regard to permissions to use the work, but did not actually prevent or limit users' ability to do so did not constitute a copy control measure under the DMCA.[23] By contrast, in a case involving CSS, the defendant attempted to argue that since encrypted DVD data could technically be copied, and the CSS system did not prevent such copying, that CSS was not a copy control measure. However, the defendant admitted that such copying is "not particularly useful" since any copy could not be accessed or viewed. The court rejected the argument, finding that notwithstanding the ability to accomplish copying of encrypted data, CSS constituted an effective copy control measure.[24]

3. What Is "Circumvention"?

Under the "access control" provisions, to "circumvent a technological measure" means "to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[25] Under the "copy control" provisions, to "circumvent protection afforded by a technological measure" means "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure."[26] Thus, both of the definitions are broad, but the definition of circumvention for access controls further assumes that the work may be scrambled or encrypted, and thus specifically calls out descrambling or decrypting as acts of circumvention.

However, not every act that bypasses a technological protection measure to gain access to or make a copy of copyrighted content constitutes "circumvention." Particularly relevant to the discussion of videogames is the status of password systems. Several cases have dealt with website passwords in the context of the DMCA and in every event found them to constitute access control measures.[27] However, these cases also established that the mere act of improperly obtaining the password (for example, from an authorized party) and using it to access content does not constitute "circumvention."

One court found that:

> circumvention requires either descrambling, decrypting, avoiding, bypassing, removing, deactivating or impairing a technological measure qua technological measure. In the instant matter, defendant is not said to have avoided or bypassed the deployed technological measure in the measure's gatekeeping capacity.

Rather, the court said that the defendant had instead merely bypassed permission to use the password, noting that "defendant did not surmount or puncture or evade any technological measure [when accessing the plaintiff's website]; instead, it used a password intentionally issued by plaintiff to another entity." While recognizing that the conduct may have been improper, it was not a violation of the DMCA.

---

[23] *Agfa Monotype Corp. v. Adobe Sys.*, 404 F. Supp. 2d 1030, 1039 (N.D. Ill. 2005)
[24] *321 Studios v. MGM Studios, Inc.*, 307 F. Supp. 2d 1085, 1097 (N.D. Cal. 2004)
[25] 17 U.S.C. § 1201(a)(3)(A).
[26] 17 U.S.C. § 1201(b)(2)(A).
[27] *I.M.S. Inquiry Mgmt. Sys., Ltd. v. Berkshire Info. Sys., Inc.*, 307 F. Supp. 2d 521, 532-33 (S.D.N.Y. 2004)

Another court similarly observed that circumvention:

> is limited to actions that 'descramble,' 'decrypt,' 'avoid, bypass, remove, deactivate or impair a technological measure.' 17 U.S.C. § 1201(a)(3). What is missing from this statutory definition is any reference to "use" of a technological measure without the authority of the copyright owner, and the court declines to manufacture such language now. As such, the court concludes that using a username/password combination as intended—by entering a valid username and password, albeit without authorization—does not constitute circumvention under the DMCA.[28]

The issue appears to be cleanly decided, until these court opinions are compared to the prior cases involving CSS. In one of the CSS cases, the defendant argued that its DVD copying software did not "circumvent" the CSS encryption (i.e. was not "avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure"), but rather simply used the authorized CSS keys to unlock the encryption. There, the Court found that "while [defendant's] software does use the authorized key to access the DVD, it does not have authority to use this key, as licensed DVD players do, and it therefore avoids and bypasses CSS." In other words, the court addressing CSS found actionable "circumvention" on precisely the same rationale that was rejected in the cases involving website passwords. The fact that CSS keys were manipulated solely by technology, while the website passwords were input by humans is a very feeble distinction.[29] As further cases develop, this tension may be resolved, with some chance that unauthorized password use may eventually be found to constitute circumvention under the DMCA.

III. DECREASING THE LEGAL RISK OF IMPLEMENTING DRM SYSTEMS

While DRM systems are an important response to piracy and are obviously strengthened by the DMCA, the issue can be highly contentious. Much has been written by critics, advocates and observers regarding the interplay between DRM technologies and the DMCA's liability regime. Content owners take the position that DRM systems and the DMCA are necessary to ensure that their rights are protected and to prevent losses due to piracy. Critics assert that DRM systems and the DMCA are overly restrictive and enable more protection than is desirable as a constitutional and policy matter.

While this debate has continued, DRM systems have nonetheless become increasingly ubiquitous and accepted by consumers of videogames and other digital media. Users are no longer surprised that their online games require authentication or that their console games are tightly managed by the platform. Yet, despite the increased acceptance, there has been a recent series of lawsuits in which users allege that they have been harmed by DRM systems. While these complaints articulate policy concerns such as unwarranted limitations on "fair use," the claims are not based on those principles. Rather, the real issues are much more practical—such as whether the user adequately consented to the particular functionalities of the DRM

---

[28] *Egilman v. Keller & Heckman, LLP*, 401 F. Supp. 2d 105, 112-114 (D.D.C. 2005)
[29] *321 Studios v. MGM Studios, Inc.*, 307 F. Supp. 2d 1085, 1098 (N.D. Cal. 2004)

technology and the accuracy of statements by content owners regarding what those systems do.

First, in late 2005, Sony BMG was accused of distributing audio CDs which installed DRM technologies on user computers without user knowledge or authorization and which posed a computer security threat. Several different DRM systems were used, all of which were alleged to install files upon the insertion of a copy-protected audio CD in the CD-ROM drive and no other action by the user. One of the systems was alleged to have installed a rootkit, which concealed running processes, files and system data. A public firestorm erupted, leading to investigation by several state attorney generals and a number of class action lawsuits.

Second, in the spring of 2006, the videogame publisher Ubisoft was accused of implementing a DRM system which compromised the security of user computers and caused permanent damage to user hardware. The system was criticized for installing its own device driver onto user computers, which was alleged to cause system instability and crashes. There were also allegations that the system caused optical CD drives to fail entirely. This dispute led to a class action lawsuit as well.

The possibility of liability arising from the manner in which DRM systems are implemented constitutes a new challenge in the evolution of this technology. Those implementing and managing DRM systems must pay close attention to the valuable lessons that these recent disputes provide.

A. Make Sure That You Have Obtained Consent If Your DRM System Manipulates User Computers

One important issue highlighted in these recent disputes is that content owners must ensure that users provide sufficient consent to manipulation of their computers by DRM technology. For example, one of the DRM systems employed by Sony BMG was claimed to have installed and launched files, including a low-level driver, before any end-user license was presented describing such technology. It was also claimed that even if the user declined the license agreement, the files nonetheless remained permanently installed. The complaint also asserted that the files were named ambiguously, making identification and removal difficult. Further, it was alleged that the software collected and transmitted information about the user's listening habits, as well information identifiable to the user's computer. Similarly, in the Ubisoft litigation, it was claimed that the DRM system replaced the user's software drivers for their CD and DVD drives, without any notice to the user. Lack of user consent to these activities was the primary focus, and because of the alleged lack of consent, the end user agreements were asserted to be invalid.

Likewise, another DRM system in the Sony BMG dispute allegedly implemented rootkit technology, installed a system drive filter driver that intercepted all calls for process, directory or registry listings and then modified what information was visible to the operating system, in order to hide every file, process, or registry key used by the DRM system. The complaint asserted that removing the technology was almost impossible, as the software was hidden, and that user attempts to manually do so risked damaging the CD drive. Also, in the Ubisoft dispute the plaintiffs alleged that drivers installed by the DRM system were "deliberately hidden from the user." User consent was at issue here as well, as there was

allegedly no disclosure that such technology was being installed or that the user system was being manipulated in these ways.

These lawsuits alleged several different forms of "damage" resulting from the implementation of these DRM systems without user consent. It was asserted that these systems interfered with or disabled users' CD and DVD drives, degraded performance and used system resources otherwise available. The DRM systems were also alleged to expose user computers to attacks by concealing files which intruders could exploit and providing access to low-level functions on the users' computers. The complaints against the Sony BMG systems even asserted that malicious programs intended to exploit the technology were already being distributed. Additionally, the automatic transfer of information about user's listening habits was alleged to injure users' expectations of privacy.

Ignoring the important issue of user consent not only poses significant risks in terms of public relations, but may expose videogame companies to potential claims as well.[30] To avoid this risk, companies must carefully plan and disclose with some precision—particularly in their end-user license agreements—the nature of the DRM technology, whether user computers are manipulated and associated risks and whether user information is collected. They should also provide accurate details regarding removal of the technology. Companies should not implement DRM technology until users agree to a license describing the technology. A number of the suits also took issue with the lack of notice on product packaging itself. These risks could have been mitigated by a very brief statement on packaging that DRM technology was implemented and directions to refer to the detailed licensing terms at a publicly accessible website.

B. Make Sure That What You Do Say About Your DRM System Is Correct

Beyond user consent and alleged "omissions," these recent disputes demonstrate how a lack of accuracy in what content owners affirmatively tell users can further complicate an already complicated issue. A number of state law claims ranging from negligent misrepresentation, deceptive acts and practices, fraud, unfair competition and false advertising, to breach of the implied covenant of good faith and fair dealing, have been premised on allegations that affirmative statements made to consumers were inaccurate.

For example, the end-user license in one recent dispute stated that "[a]s soon as you have agreed to be bound by the terms and conditions of the EULA, this CD will automatically

---

[30] There are a number of legal theories that have been relied on in these recent cases. Plaintiffs have asserted claims under the federal "Computer Fraud and Abuse Act" which imposes liability on (a) one who intentionally accesses a computer without authorization or exceeds authorized access, to obtain information from any protected computer knowingly or (b) one who, with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value. Negligence and "deceptive acts and practices" claims under various state laws, such as California's Consumer Legal Remedies Act, were based on lack of consumer consent as well. More generally, the California Supreme Court has recognized that the common law tort of trespass could encompass simple unauthorized electronic contact with a computer system when it causes damage or impairment of the system. *See Intel v. Hamidi*, 30 Cal. 4th 1342 (2003).

install a small proprietary software program. . .," when in fact the DRM software was installed before the license was accepted. One content owner stated regarding its DRM system that it "does not interfere with or impact any of the normal operations and/or functions of your computer." Plaintiffs asserted that this was untrue because the system installed and replaced low-level system drivers affecting the functions of the user's hardware. Likewise, one defendant stated in its license, on its website and in other public statements that "the software will not be used at any time to collect any personal information from you, whether stored on your computer or otherwise." Plaintiffs, however, alleged that the DRM software automatically collected information identifying the album the user was playing and information identifiable to their computer and pointed out the creator of the system even marketed it for this purpose. Thus, it was difficult to explain statements that no user information was collected.

Clearly, content owners must be careful in describing their DRM systems. The impulse to downplay DRM technology, to gain the confidence of users, is understandable. However, if plaintiffs are able to cast statements or representations made by content owners as inaccurate or untruthful, that strategy poses unacceptable risk. Moreover, once a dispute arises regarding DRM technology, missteps in dealing with the challenge may compound the problem as illustrated by defendants' statements and actions in the recent litigation. For instance, one content owner insisted that the system "does not compromise security" while at the same time distributing uninstallers which allegedly either did not uninstall the DRM software or installed control software which could be accessed and executed by malicious websites. These statements were made even after the Department of Homeland Security noted that the technology can "pose a security threat" and one uninstallation procedure "introduces vulnerabilities to a system." Rather than helping to resolve the difficulties, these statements became allegations in the complaint.

Obviously, these are difficult issues and the content owners involved in these recent disputes were certainly taken by surprise. But, the cases bring needed attention to some neglected issues and provide an excellent opportunity for others to avoid making the same mistakes. Generally, the solution lies in complete communication with users, avoiding the inclination to de-emphasize the effects of DRM technology and implementation of a clear plan regarding licensing terms and public statements. Videogame companies must pay attention to these matters, to ensure that the full potential of DRM systems to protect valuable content is realized.