MODEL ANSWER

Instructions

This examination consists of a single essay question. You have 24 hours after picking up the exam from the Registrar to compose your answer (preferably typed or printed from a computer) and return both the exam and your answer to the Registrar. Your answers must be limited to 10 double-spaced typed pages, 1-inch margins, 12-point type (or roughly 3000 words).

You are not permitted to discuss any aspect of the problem or any issue raised by the problem with other people, whether or not class members, but you are permitted to use or refer to any materials you like in composing your answer. You may not cite as authority for any proposition of law anything that is not found in the textbook, any class handout materials, your class notes, or the materials found at the Course Materials page or Syllabus of the class web site. In other words, if you know of a case that we did not study but that you think is dispositive of an issue, you will get no points for saying “Under the principle of A v. B, issue 1 must be decided in favor of X.” However, you may use the reasoning of A v. B and apply that, preferably with your own improvements, to the fact situation in the problem. In my opinion, an A++ answer can be written based solely on the materials that we have studied, and I would advise wasting no time looking for other cases or materials.

GOOD LUCK!
Problem

SafeNetworks, Inc. (SN) produces a group of related software products designed to allow digital distribution of copyright protected works (including music and video in digital format) while allowing the copyright owner to control subsequent copying and distribution of those works. SafeProducer is a software product (computer program) that encodes works in digital format into a special, and assertedly proprietary, “SafeMedia” format. SafeServer is a software product that takes a work so encoded and allows delivery of that work from internet web sites (e.g., sites operated by the copyright owner of the encoded content). Delivery from SafeServer is through so-called “streaming,” with which a user clicks on an appropriate icon at the server site and the work is immediately delivered in audio, visual, or audiovisual form, as appropriate. To receive such streamed content delivered through SafeServer, however, the user must have installed on her computer another SN product called SafePlayer. (If content in SafeMedia format is made available from a web site not using SafeServer, it is essentially free for copying or further distribution, just like any other digital file.)

It is the interaction between SafePlayer and the signals emanating from SafeServer that allow the control sought by many copyright owners. This control has two aspects: First, SN has constructed SafeServer and SafePlayer so that they engage in a “secret handshake” when streaming delivery is requested. This secret handshake is an authentication sequence, the precise nature of which is heavily guarded by SN. Unless authentication takes place as a result of a successful secret handshake, streaming does not begin. Moreover, the copyright owner making use of SafeServer may also choose to set a “Copy Switch” on or off. When the Copy Switch is off, the streamed content can be saved to the hard drive of the person initiating the streaming. When the Copy Switch is on, however, SafeServer so instructs SafePlayer and SafePlayer does not allow the streamed content to be saved. Content owners can also arrange using this “SafeSystem” technology to enable users to listen to music or view video content on a “pay per play” basis that requires payment each time the end user wishes to hear or view the work in question.

SN’s business plan is to distribute SafePlayer widely and without charge through internet downloads. SN customer service also supports users of SafePlayer who have technical difficulties with installation or operation. SN makes its money by licensing SafeProducer and SafeServer to content owners who seek the security from copying that the SN “SafeSystem” provides. SafePlayer is by far the most widely adopted player by computer users, with estimates that it is installed on over 80% of all personal computers in the United States. Because of its wide installation base, content owners are more strongly inclined to license SafeProducer and SafeServer from SN than to use similar products from other companies.
Flowbox, Inc. now offers a software product called “Net VCR.” Net VCR allows the personal computer user to record streamed content from the internet much in the way an ordinary video cassette recorder captures the contents of broadcast or cable signals. Net VCR can “understand” all of the open formats in which content is embodied, such as WAV, MP3, and WMA. However, Flowbox was able to reverse engineer the SafeSystem “secret handshake,” and as a result Net VCR can also receive streamed content delivered from SafeServer. Flowbox advertises Net VCR as having the “ability to accept SafeMedia files as easily as you would any other file, without the need to use SafePlayer.” Flowbox does not expressly state in its advertising that use of Net VCR, instead of SafePlayer, will allow the user to make copies of the streamed audio or video content, but knowledge of this general ability has been spreading among the bloggers and others and is now fairly widespread.

SN brings an action against Flowbox, charging violation of the DMCA. You are clerk to the judge who must decide the case. The judge asks you to give her a memo on the legal and policy issues raised by these facts, without concentrating on the specific charges in the complaint. She does want you to consider, however, at least the following issues:

(1) Does SN have standing to bring a DMCA claim? (See Section 1203(a) of the Copyright Act.)

(2) Assuming SN does have standing, what potential claims might it have under the DMCA? Would any of the analysis change if it could be shown that, technologically, Net VCR could fairly easily be designed to respect the “Copy Switch” choice made by the content owner while still allowing the streaming content from SafeServers to be played on Net VCR?

(3) Does Flowbox have any defenses under the DMCA (or otherwise)?

Please draft such a memo. You may assume that the reader knows all relevant statutes and cases, so language from either should be brought in only in the service of specific arguments.

Model Answer

(1) SN is charging Flowbox with a violation of § 1201. Section 1203 says, “Any person injured by a violation of section 1201 . . . may bring a civil action . . . .” Let us assume that Net VCR is a device whose distribution would violate § 1201(a)(2) or 1201(b). How has SN been injured by Flowbox’s distribution of Net VCR? SN is not a content owner whose work has been accessed or copied, unless we take the view that Net VCR gives “access” to the functionality of RealServer. Access to this functionality does not give access to RealServer in the sense that RealServer becomes available for copying and further distribution. It only allows using
RealServer’s functionality to access the content of the works belonging to SN’s content-owner customers. Access of this type is generally available by anybody through SafePlayer, at least with conditions (such as not copying if the Copy Switch is set). We are assuming here that § 1201 is violated here with respect to content distributed via SafeServer. SN will argue that its business is injured severely if its customers cannot rely on the protections SafeSystem is designed to give them, and these assumed § 1201 violations by Flowbox will jeopardize such customer reliance. Is this the kind of injury that § 1203 is designed to prevent?

It is clear that Congress was worried about the increased ease of piracy as copies of works in digital format became available on the internet. SafeSystem is an attempt to place access and copying of works behind a defensive technological wall. Had any given content owner created the system, he would have standing to sue for circumvention acts or devices that violate the DMCA. It seems more efficient to allow the content owners to allow others more skilled in antipiracy protection methods to develop them for use by content owners, which appears to be what has occurred here. To deny standing to SN might weaken the enforceability of the DMCA, because individual content owners are not necessarily as sufficiently well organized as the movie studios in Remeirdes to band together to bring a claim, and individually the their damages may not be high enough. While such individual content owners may sue Flowbox now, making these same claims, I conclude that “injury” in section 1203 is sufficiently broad to encompass what has happened, or might potentially happen, to SN’s business here to allow them to bring the claim. We may wish to reconsider this point when we look more closely at the nature of SN’s business plan.

(2) Nothing in the facts indicates that Flowbox itself infringed any copyrights or circumvented any access or copy control measures. The question is whether Flowbox violated the anti-trafficking provisions of 1201(a)(2) or 1201(b)(1).

Works distributed through SafeServer are designed to be decrypted solely by SafePlayer, which in turn respects the anticopying choice of the content owner, if such choice has been made. Is SafeSystem a technological measure that effectively controls access to a work? It does not control access to the work in streaming form, because SafePlayer is widely available to anyone, who can download it without cost and play on it any work distributed through SafeServer. The Federal Circuit in Chamberlain reasoned that circumventing access controls to reach the functionality of a computer program was not a DMCA violation because none of the evils against which the DMCA was designed to protect were implicated unless access also gives the ability to copy. Here, by failing to respect the Copy Switch function of SafeSystem, Net VCR does, in fact, supply the ability to copy. Consequently, under the reasoning of Chamberlain, Net VCR does supply access to a work that is protected by a technological measure (the “secret handshake”) by either reproducing the secret handshake or circumventing it. The facts do not indicate which way was used. If Flowbox simply reproduced the “keys” to the secret handshake
without copying any other code from SN’s programs, the question is whether Net VCR “circumvents” the technological measure. At least one case has held that using an authorized password without authorization is not circumvention within the meaning of the DMCA. On the other hand, Remeirdes and other cases have concluded that using decryption means to get intelligible access to an encrypted work is circumvention if done without authorization. This approach has the disadvantage that the key to any 1201 violation is lack of authority, which means that circumvention of even the most rudimentary protection system would lead to DMCA liability, which raises the question of why Congress would place so much emphasis on “technological measures that effectively control” access or copying in the Act.

Another way to deal with the access issue is simply to divorce access from copying and ask whether the technological measure effectively does control access in a meaningful way. In this case, if we put the Copy Switch to one side for the moment, Net VCR provided exactly the same access to the protected content that SafePlayer itself provides. SafePlayer is available to anyone who wishes to download it, at no cost. I conclude, therefore, that SafeSystem does not effectively control access to the protected content distributed through SafeServer and that § 1201(a)(1) is therefore not violated.

Section 1201(b)(1), however, is another story. Here the failure to respect the Copy Switch by Net VCR becomes crucial. The “access” permitted by SafePlayer does not allow digital copying of the content, whereas the access supplied by Net VCR does. The Copy Switch, when used in conjunction with SafeSystem, is a technological measure that prevents copying of protected content, because in its ordinary operation those two features operate in tandem to protect the copyright owner’s right of reproduction. We must therefore inquire into whether Net VCR is primarily designed for, has only a limited commercially significant purpose other than, or is marketed by Flowbox for use in circumventing such copy-control protection.

Here the evidence is unclear. Flowbox was arguably designed as competition to SafePlayer in the market for software products that can receive streaming content. Generally speaking, competition in such markets is something the law wants to promote, not inhibit. If Net VCR’s system respected the Copy Switch setting chosen by the content owner, then even under the Federal Circuit’s definition of “access” there would be no violation of § 1201(a)(2), and because no digital copying is permitted when that setting is respected, there would be no violation of § 1201(b)(1), either. It may be that Flowbox was unable to reproduce a product that respected the Copy Switch, or that it was merely indifferent to reproducing SafePlayer’s functionality to that extent.

Does Net VCR have only a limited commercially significant purpose other than circumvention of SafeSystem’s copy controls? It does exist as competition for SafePlayer, but would Flowbox have made and offered it to the public in a form that maintained the Copy
Switch? To the extent that Net VCR does respect the Copy Switch, it does the same thing as SafePlayer, so SN will argue that it has no commercially significant purpose other than copy control circumvention. But Net VCR understands all of the formats that are used to distribute content on the internet, whether through SafeServer or not. That is arguably a commercially significant purpose – one that makes internet use easier for consumers by allowing them to use a single “playback” product for all of the streamed content they find on the internet. That it also circumvents the Copy Switch would not be relevant if this other purpose is of more than limited commercial significance.

Is Net VCR marketed for use in copy control circumvention? Again, the evidence so far is ambiguous. Flowbox does not advertise that its use will allow making copies of streamed content that cannot be effected using SafePlayer, but it is surely aware that others are making that argument on its “behalf.”

At trial the court will need more evidence on these aspects of Net VCR’s design. And that raises the question of who has the burden of proving what. In particular, if it can be shown by SN that Net VCR could easily be designed so that it would respect the Copy Switch, Flowbox would have to show that it had some legitimate reasons for leaving it out of the design other than to add illegal circumvention technology to an otherwise useful and legal device.

(3) As for defenses, the most likely defense to a DMCA violation is that under 1201(f) for reverse engineering. Net VCR must include some software that allows playing of streamed content. There is nothing in the facts to indicate that Flowbox copied any of the code from SafePlayer or any other SN software. So, it appears that Net VCR contains an “independently created computer program” that Flowbox sought to make compatible with content streamed through SafeServer. Is that content a “computer program”? In normal parlance, the streamed content is more like a letter or article written on a word processor and saved in a file. However, the statute defines a computer program to be a set of statements or instructions that cause a computer to achieve a certain result. Here, the streamed digital file causes the recipient’s computer to play the streamed work, so arguably it’s a set of statements or instructions used in a computer to achieve that result.

“Interoperability” is defined in 1201(f)(4) as “the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.” Net VCR seeks to accept the streamed digital content from a SafeServer site in SafeMedia format and perform the audiovisual content in real time, just as SafePlayer does. It supplies information to the SafeServer file (at a minimum, the “secret handshake”) and it takes information from that file, namely, the digital content of the file. It “uses” the information it has received by performing the work so streamed on the user’s computer. Therefore, if such streamed content is a computer program, Flowbox is seeking compatibility of its Net VCR
software with those “other programs”, and any act of circumvention of the technological measures protecting SN’s SafeSystem software would be justified under 1201(f)(1). Section 1201(f)(2) allows an exemption from the antitrafficking provisions of 1201(a)(2) and (b) in order to enable the reverse engineering analysis permitted by 1201(f)(1). That does not seem to be directly applicable to these facts. However, 1201(f)(3) permits the information derived from reverse engineering activities permitted under (f)(1)&(2) to be made available to others, provided it is made available “solely for the purpose of enabling interoperability of an independently created computer program with other programs,” and provided that copyright law is not otherwise infringed in the process. Here the information on the “secret handshake” is given to consumers in the form of Net VCR, allowing them to play content streamed through SafeServer with independently created software, namely, the software included in Net VCR. It therefore seems that Flowbox has a good argument under 1201(f) that manufacture and distribution of its Net VCR does not violate 1201(a)(2) or (b) because of the reverse engineering exemption.

SN might argue in response that, by failing to design Net VCR so that it respects the Copy Switch in the streamed content, it is not “compatible” with the SafeServer software. This is an interesting argument and one that has not been addressed by the courts. Does “compatibility” mean that a reverse engineer is allowed to work only if she achieves 100% compatibility, or at least as much compatibility as she is capable of achieving? Would the result in Remeirdes have been different had Jon Johansen or those following him designed their DeCSS program so that it could play DVDs but would not permit copying them? Allowing competition at the level of playback devices seems well within the spirit of the DMCA, which is aimed at stopping piracy on the internet. By respecting anti-copying measures taken by the content owners, the defendants are not engaged in any activity that the DMCA was designed to control.

If we hold that § 1201(f) is available only to those who achieve 100% compatibility, we run the risk that courts will have to look in detail at the technical measures taken by reverse engineers and at their individual competence. There may also be tradeoffs between 100% compatibility and additional technological advances that a particular reverse engineer might have to make. How can a court decide whether those tradeoffs are within or without the “spirit” of the DMCA? On balance, I would say that Flowbox used reverse engineering permitted under 1201(f) to build its competitive playback device Net VCR, because “compatibility” generally means accepting and being able to interoperate with the incoming streamed content in a manner that is intelligible to the user. In ordinary language, most people would say that Net VCR is “compatible” with SafeServer, and “interoperability” within the meaning of the reverse engineering exemption generally means that the independently created program is able to accept the functionality of the program with which it seeks to interoperate. Net VCR does that, even though it does not make use of the entirety of SafeServer’s software functionality. It is a very close call, however.

Does Flowbox have any other defenses? Availability of the reverse engineering exemption depends on use of the interoperability information without any copyright
infringements. Flowbox might well be charged with contributory infringement by distributing a device that facilitates the illegal copying of protected content. The problem that SN has in asserting this claim is the *Sony* case, which says that the distribution of a device that has a substantial noninfringing use is not contributory infringement, even where the device manufacturer knows that at least some users will use the device to infringe. The *Napster* and *Aimster* cases appear to narrow *Sony* somewhat, but both of those cases are distinguishable in that the defendants had ongoing control over what users of their product were doing. Here, as in *Grokster* and *Sony*, Flowbox has no control over what its users do with Net VCR after it is installed on the users’ computers. Moreover, Flowbox does have a substantial noninfringing use, namely, playing streamed content from SafeServer, the streaming of which (if not the copying) has been authorized by the copyright owner. On the other hand, Flowbox has designed its device in such a way that it does not respect the Copy Switch. It knows, at least now and probably from the beginning, that some users would use Net VCR to store (i.e., copy) files of protected works on their hard drives. Especially if it is easy for Flowbox to modify its technology to respect the Copy Switch, and maybe even if it is not so easy but possible, it does not seem unreasonable for a court to require that modification, reluctant though we should be to get the courts into the business of writing technological specifications. Given the closeness of the case for the 1201(f) exemption anyway, this seems like a reasonable compromise. The other choice would be to deny the exemption altogether, which would leave the Net VCR technology completely unavailable.