08-732 Law of Computer Technology, Prof. Shamos
Homework 3. Due Wednesday, November 22, 2017, 11:59 p.m.

For the policy on homework, consult Homework 1.

Your homework file should be named [LastName][FirstName].doc (example: ShamosMichael.doc) and your name should also appear at the top of the first page. Your file should be submitted through Canvas.

Do both problems 1 and 2.

1. Copyrights [60 points].

CMU Professor Blackhat teaches 15-666, a course on "Ethical Hacking." Part of the course is intended to teach students about security vulnerabilities in commercial software, particularly computer games. Many games come on DVDs containing data on tracks that consumer DVD burners cannot write. Therefore, if you simply make a copy of a game DVD on your PC, the copy will not run because data on the hidden unwritable tracks will be missing. Blackhat maintains a laboratory with an industrial DVD burner of the type used by game manufacturers. This burner will easily make working copies of game DVDs because it is able to write to the entire DVD.

To allow the students to study data security techniques, Prof. Blackhat makes copies of the encrypted DVD of the game Apocalypse, manufactured by FinalCorp[1]. He makes one copy for each student in the class. When students come to the lab, he hands out the DVDs to them. Before they leave the room they must return the DVDs to Blackhat. He is very strict about this. While they are in the lab, they are encouraged to try to break the DVD security mechanisms on their own PCs. One of the students, Chad Cheater, succeeds. He writes some code, which he calls BreakDisk, which will allow anyone to run a copy of Apocalypse made on a regular consumer burner (which means it doesn't have the normal data on hidden tracks as distributed by FinalCorp).

When sales of Apocalypse suddenly go down in Pittsburgh, FinalCorp investigates and discovers everything that has been going on. FinalCorp brings a lawsuit against CMU, Blackhat and Cheater in Federal court in the Western District of Pennsylvania (Pittsburgh).

a. FinalCorp asserts that Blackhat's copying of the Apocalypse DVDs is a copyright infringement. He made copies without FinalCorp's authorization. Blackhat says it was a fair use under 17 U.S.C. §107 because the copies were only for classroom use and were collected after every class. Furthermore, they were for use in security research. FinalCorp responds that there is no fair use of software in this manner because of the Computer Software Copyright Amendments, 17 U.S.C. §117. Blackhat says CMU is a

[1] "Apocalypse" and "FinalCorp" are fictional, as is Prof. Blackhat. 15-666 really exists, and is entitled "Computer Game Programming," but the descriptions in this homework have no relation to the actual course.

non-profit education institution and is allowed to loan software under 17 U.S.C. §109 because he attached to the DVDs the notice required under 37 C.F.R. §201.24.

b. FinalCorp asserts that Blackhat's copying of the Apocalypse DVDs violates the Digital Millennium Copyright Act (DMCA), 17 U.S.C. 1201(a) because Blackhat circumvented FinalCorp's protection mechanism that was supposed to prevent copying the DVDs. Blackhat says he was teaching reverse engineering encryption and claims the specific exemptions for reverse engineering and encryption research in 17 U.S.C. §1201(f) and (g).

c. FinalCorp says that, by succeeding in defeating its protection mechanism, Cheater violated the anti-circumvention provision of the DMCA, 17 U.S.C. 1201(a). Cheater says that the work was done as part of a class on security research and also claims the exemptions in 17 U.S.C. §1201(f) and (g).

d. FinalCorp says that, by distributing BreakDisk, Cheater violated the anti-trafficking provision of the DMCA, 17 U.S.C. §1201(a)(2). Cheater says that BreakDisk does not work on authorized copies of Apocalypse (because BreakDisk first checks to see if the DVD copy is authorized and will not run if it is). BreakDisk only operates on unauthorized copies and therefore it does not circumvent a "technological measure that effectively controls access to a work."

QUESTION 1: Evaluate each of the arguments in (a)-(d). Determine who is legally correct in each part of the question and explain your answer. If you address fair use, you must carefully analyze each of the four statutory fair use factors. You should not need any additional facts, but if you feel you do, make a reasonable assumption and state what assumption you are making.

The relevant statutes are reproduced at the end of this document.

2. The Twitter Patents [60 points].

Twitter, Inc. owns 57 patents and has applied for another one. You can view one of its patent applications here. You do not need to read the whole document. The application does not mention the word "tweet," but the invention is a method for prioritizing tweets ("messages") according to a score value based, for example, on who is following a particular user.

Claim 1 reads,

1. A computer-implemented method inserting messages in a message sharing system, comprising:
[a] receiving electronic messages posted by a plurality of posting users;
[b] receiving interaction information for each of the electronic messages, the interaction information comprising an indication of at least one of information within the electronic

message, a posting user of the electronic message and a following user of the electronic message;
[c] determining a score for each electronic message based on the interaction information for the electronic message;
[d] selecting, based on the determined scores, one or more electronic messages for insertion into a message stream of a user; and
[e] transmitting the selected electronic messages to the user for insertion into the message stream of the user.

If patented, this claim would be very valuable because it covers, for example, selecting messages based on relevance scoring and can be used as a way of presenting advertising, which is the primary business model of Twitter, Google, Facebook and others.

Google, for example, says that claim 1 reads on an ordinary Google search because:
1. Users share information by posting web pages, which Google indexes so people can retrieve them. This forms a message sharing system in which the shared messages are web pages.
[a] Google receives web pages, which are electronic messages, posted by a plurality of users when it spiders the Web.
[b] Google obtains keyword information about web pages, which is information within the page. Google also obtains linking information about which other web pages link to a web page, which is information about a "following user" of the web page. A "following user" is someone who links to the web page being followed.
[c] Google determines a score for each web page based on the information obtained in [b]. This is Google's famous PageRank algorithm.
[d] Google determines a subset of web pages based on their PageRank scores, to present to a user in response to a query (a page of search hits)
[e] Google transmits a sequence of ranked search hits to the search user. The "message stream of the user" is the HTML page of hits that Google sends to the user's browser.

Note: the patent application eventually issued as U.S. Patent 9,356,806 on May 31, 2016, but with very different claims.

QUESTION 2:
(a) Assume that Google searching and PageRank are prior art as to the Twitter application, which was filed in 2010. (Google and PageRank are much older than that.) Does claim 1 "read on" a Google search as Google asserts? In other words, is claim 1 invalid because it claims part of the prior art? You must give a full explanation of your answer. Just saying "yes" or "no" is worth ZERO.

(b) Facebook is also concerned about the Twitter application. Facebook argues that claim 1 (i) is not "tied to a particular machine or device"; (ii) does not transform any tangible thing into a different states; and (iii) claims no more than the abstract idea of transmitting messages based on a "score." Therefore, Facebook insists that claim 1 is an unpatentable business method. Facebook says that merely stating that the method is "computer-implemented," without explaining which portions of the process, if any, are actually

performed by computer, does not tie the claim to a machine. It further says that all the steps of claim 1 could be performed by a human sending telegrams or text messages and does not require a computer at all. Does claim 1 fall into one of the four categories of patentable subject matter, namely process, machine, manufacture or composition of matter, or it is unpatentable subject matter? Relevant to this question is the *Alice* case listed on the course web page. You may also want to consult DDR Holdings, LLC v. Hotels.Com, L.P. (Fed. Cir., Dec. 5, 2014). You must address each one of Facebook's arguments.

STATUTORY APPENDIX

FAIR USE:

17 U.S.C. §107 - Limitations on exclusive rights: Fair use

Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include—

(1) the purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes;

(2) the nature of the copyrighted work;

(3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and

(4) the effect of the use upon the potential market for or value of the copyrighted work.

17 U.S.C §109 - Limitations on exclusive rights: Effect of transfer of particular copy or phonorecord

(a) Notwithstanding the provisions of section 106(3), the owner of a particular copy … lawfully made under this title, or any person authorized by such owner, is entitled, without the authority of the copyright owner, to sell or otherwise dispose of the possession of that copy.

(b)(1)(A) Notwithstanding the provisions of subsection (a), unless authorized by the owners of copyright in the sound recording or the owner of copyright in a computer program (including any tape, disk, or other medium embodying such program), and in the case of a sound recording in the musical works embodied therein, neither the owner of a particular phonorecord nor any person in possession of a particular copy of a computer program (including any tape, disk, or other medium embodying such program), may, for the purposes of direct or indirect commercial advantage, dispose

of, or authorize the disposal of, the possession of that phonorecord or computer program (including any tape, disk, or other medium embodying such program) by rental, lease, or lending, or by any other act or practice in the nature of rental, lease, or lending. The transfer of possession of a lawfully made copy of a computer program by a nonprofit educational institution to another nonprofit educational institution or to faculty, staff, and students does not constitute rental, lease, or lending for direct or indirect commercial purposes under this subsection.

(b)(1)(B) This subsection does not apply to—
(i) a computer program which is embodied in a machine or product and which cannot be copied during the ordinary operation or use of the machine or product; or
(ii) a computer program embodied in or used in conjunction with a limited purpose computer that is designed for playing video games and may be designed for other purposes.

COMPUTER SOFTWARE COPYRGHT AMENDMENTS:
17 U.S.C. §117 - Limitations on exclusive rights: Computer programs
(a) Making of Additional Copy or Adaptation by Owner of Copy.—Notwithstanding the provisions of section 106, it is not an infringement for the owner of a copy of a computer program to make or authorize the making of another copy or adaptation of that computer program provided:
(1) that such a new copy or adaptation is created as an essential step in the utilization of the computer program in conjunction with a machine and that it is used in no other manner, or

(2) that such new copy or adaptation is for archival purposes only and that all archival copies are destroyed in the event that continued possession of the computer program should cease to be rightful.

(b) Lease, Sale, or Other Transfer of Additional Copy or Adaptation.—
Any exact copies prepared in accordance with the provisions of this section may be leased, sold, or otherwise transferred, along with the copy from which such copies were prepared, only as part of the lease, sale, or other transfer of all rights in the program. Adaptations so prepared may be transferred only with the authorization of the copyright owner.

DIGITAL MILLENNIUM COPYRIGHT ACT:
17 U.S.C. §1201(a) Violations Regarding Circumvention of Technological Measures.—
(1) (A) No person shall circumvent a technological measure that effectively controls access to a work protected under this title.

(2) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—

(A) is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a work protected under this title;

(B) has only limited commercially significant purpose or use other than to circumvent a technological measure that effectively controls access to a work protected under this title; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing a technological measure that effectively controls access to a work protected under this title.

(3) As used in this subsection—
(A) 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; and

(B) a technological 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.

(b) Additional Violations.—
(1) No person shall manufacture, import, offer to the public, provide, or otherwise traffic in any technology, product, service, device, component, or part thereof, that—
(A) is primarily designed or produced for the purpose of circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof;

(B) has only limited commercially significant purpose or use other than to circumvent protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof; or

(C) is marketed by that person or another acting in concert with that person with that person's knowledge for use in circumventing protection afforded by a technological measure that effectively protects a right of a copyright owner under this title in a work or a portion thereof.

(2) As used in this subsection—
(A) to "circumvent protection afforded by a technological measure" means avoiding, bypassing, removing, deactivating, or otherwise impairing a technological measure; and

(B) a technological measure "effectively protects a right of a copyright owner under this title" 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.

(c) Other Rights, Etc., Not Affected.—
(1) Nothing in this section shall affect rights, remedies, limitations, or defenses to copyright infringement, including fair use, under this title.

(2) Nothing in this section shall enlarge or diminish vicarious or contributory liability for copyright infringement in connection with any technology, product, service, device, component, or part thereof.

(f) Reverse Engineering.—
(1) Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.

(2) Notwithstanding the provisions of subsections (a)(2) and (b), a person may develop and employ technological means to circumvent a technological measure, or to circumvent protection afforded by a technological measure, in order to enable the identification and analysis under paragraph (1), or for the purpose of enabling interoperability of an independently created computer program with other programs, if such means are necessary to achieve such interoperability, to the extent that doing so does not constitute infringement under this title.

(3) The information acquired through the acts permitted under paragraph (1), and the means permitted under paragraph (2), may be made available to others if the person referred to in paragraph (1) or (2), as the case may be, provides such information or means solely for the purpose of enabling interoperability of an independently created computer program with other programs, and to the extent that doing so does not constitute infringement under this title or violate applicable law other than this section.

(4) For purposes of this subsection, the term "interoperability" means the ability of computer programs to exchange information, and of such programs mutually to use the information which has been exchanged.

(g) Encryption Research.—
(1) Definitions.—For purposes of this subsection—

(A) the term "encryption research" means activities necessary to identify and analyze flaws and vulnerabilities of encryption technologies applied to copyrighted works, if these activities are conducted to advance the state of knowledge in the field of encryption technology or to assist in the development of encryption products; and

(B) the term "encryption technology" means the scrambling and descrambling of information using mathematical formulas or algorithms.

(2) Permissible acts of encryption research.—Notwithstanding the provisions of subsection (a)(1)(A), it is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research if—
(A) the person lawfully obtained the encrypted copy, phonorecord, performance, or display of the published work;

(B) such act is necessary to conduct such encryption research;

(C) the person made a good faith effort to obtain authorization before the circumvention; and

(D) such act does not constitute infringement under this title or a violation of applicable law other than this section, including section 1030 of title 18 and those provisions of title 18 amended by the Computer Fraud and Abuse Act of 1986.

(3) Factors in determining exemption.—In determining whether a person qualifies for the exemption under paragraph (2), the factors to be considered shall include—
(A) whether the information derived from the encryption research was disseminated, and if so, whether it was disseminated in a manner reasonably calculated to advance the state of knowledge or development of encryption technology, versus whether it was disseminated in a manner that facilitates infringement under this title or a violation of applicable law other than this section, including a violation of privacy or breach of security;

(B) whether the person is engaged in a legitimate course of study, is employed, or is appropriately trained or experienced, in the field of encryption technology; and

(C) whether the person provides the copyright owner of the work to which the technological measure is applied with notice of the findings and documentation of the research, and the time when such notice is provided.

37 C.F.R. §201.24
Warning of copyright for software lending by nonprofit libraries.
(a) Definition. A Warning of Copyright for Software Rental is a notice under paragraph (b)(2)(A) of section 109 of the Copyright Act, title 17 of the United States Code, as amended by the Computer Software Rental Amendments Act of 1990,

Public Law 101–650. As required by that paragraph, the ''Warning of Copyright for Software Rental'' shall be affixed to the packaging that contains the computer program which is lent by a nonprofit library for nonprofit purposes.

(b) Contents. A Warning of Copyright for Software Rental shall consist of a verbatim reproduction of the following notice, printed in such size and form and affixed in such manner as to comply with paragraph (c) of this section.

Notice: Warning of Copyright Restrictions

The copyright law of the United States (title 17, United States Code) governs the reproduction, distribution, adaptation, public performance, and public display of copyrighted material. Under certain conditions specified in law, nonprofit libraries are authorized to lend, lease, or rent copies of computer programs to patrons on a nonprofit basis and for nonprofit purposes. Any person who makes an unauthorized copy or adaptation of the computer program, or redistributes the loan copy, or publicly performs or displays the computer program, except as permitted by title 17 of the United States Code, may be liable for copyright infringement. This institution reserves the right to refuse to fulfill a loan request if, in its judgement, fulfillment of the request would lead to violation of the copyright law.