CPSC 457/557 // Fall 2011 // Answer Key for Exam 1

Many of the answers below are just examples of correct answers to the exam questions. Credit was given for all correct answers, regardless of whether they appear in this answer key. Furthermore, a few of these answers are considerably longer and more detailed than answers needed to be to earn full credit; the additional information is provided so that anyone who answered a question incorrectly can read a full explanation of what the question was getting at.

Question 1

(a) In the digital world, "access is by copying." Numerous copies are made in the course of "normal use" of a copyright work in digital form, but this exclusive right granted by copyright law was never intended to govern normal use of a work by a user who had accessed the work lawfully. Rather, the granting of this exclusive right assumed that copying was a good proxy for infringement – something that copying simply is not in the context of digital works. See, *e.g.*, page 28ff of http://zoo.cs.yale.edu/classes/cs457/fall11/Overview.pdf for a more detailed discussion.

(b) In principle, DRM systems could force people to use copyright works only in ways that rights holders approve of. In particular, they could make it technologically infeasible for users to do things that are universally considered fair use. If such uses never occurred, no one would ever be sued for infringement after having made such a use, and the fair-use defense would never be needed. In this scenario, the whole fair-use doctrine would be useless. There is no equivalent technological scenario in the analog world.

(c) The First Sale Rule gives the lawful owner of a particular copy of a copyright work, such as a book or a CD, the right to dispose of that copy however he chooses; he may, for example, resell the copy, give it away, or lend it to friends or colleagues. Because it enables used-book stores, used-record stores, public libraries, and other forms of re-use of works without permission of the copyright owner, the First Sale Rule has served a tremendously valuable social purpose. It is clear how to apply the rule when copies of works are embodied in physical objects: The owner of the copy possesses a physical object that he can sell, lend, or otherwise dispose of as he pleases. Moreover, giving the owner of a copy permission to dispose of this object does not give him permission to make additional copies or to distribute them; thus, the First Sale Rule does not vitiate the copyright owner's exclusive rights. In the digital world, however, "content has been liberated from medium." (See page 10ff of http://zoo.cs.yale.edu/classes/cs457/fall11/Overview.pdf for a short discussion of that phrase.) The natural way (and, in a purely technical sense, the only way) for the owner of a digital copy to sell, give, or lend that copy to someone else is by making *another* perfect digital copy and transmitting it to that other person's computer. Such an act of copying and transmission results in *both* parties' possessing copies of the work and demonstrates an inherent tension between the first-sale rule and the copyright owner's exclusive rights. One could insist on ubiquitous DRM systems that erased a digital copy from one owner's computer

when the copy is "given" or sold to another owner or temporarily disabled access on a lender's computer until the borrower "returned" the copy, but we have already acknowledged that DRM systems are distasteful to many users and often deeply technically flawed. More importantly, this approach is tantamount to simulating analog usage in a digital environment; given that digital works have zero marginal cost of production and distribution, whereas analog works have positive marginal cost, simulation of this sort prevents our society from realizing a significant portion of the economic and social promise of digitization.

(d) [This question was actually supposed to be about exceptions to the prohibition on circumvention, not to the prohibition on distribution of circumvention tools. Some people answered the former question anyway. Full credit was given for a correct answer to either question.]
A much-discussed exception to the prohibitions on circumvention and on the development and distribution of circumvention tools is the "encryption-research" exception. See page 327ff of http://zoo.cs.yale.edu/classes/cs457/fall11/DMCA.pdf for a detailed discussion of this exception. It is hard to apply and enforce fairly for many reasons, among them the implication that a circumventor must be formally trained and/or employed as an "encryption researcher," enrolled in a formal course of study of encryption, or able to publish his or her results in an official scientific journal or conference proceedings. In reality, many important insights into the security (or lack thereof) of DRM systems are provided by amateur tinkerers who circulate their findings on blogs and in chat rooms rather than in journals and conference proceedings.

Question 2

No. As explained by Halderman and Felten, commercial DRM systems are not designed primarily to enforce copyright law and to support users who wish to comply with it. Rather, they are designed to serve the interests of content distributors and DRM vendors. Content distributors want primarily to limit the number of unauthorized copies that users can make, because they assume that limitations of this sort will increase the number of copies that are purchased. DRM vendors, on the other hand, wish to have their systems installed on as many computing platforms as possible; if users find a particular DRM system overly restrictive, annoying, or privacy-invasive, vendors of computing platforms will be reluctant to install it.

Question 3

(a) iii: WIPO
(b) DMCA
(c) ACTA's anti-circumvention requirements are similar to those of the DMCA: It forbids "unauthorized circumvention of an effective technological measure carried out knowingly or with reasonable grounds to know" and "the offering to the public by marketing of a device or product, including computer programs, or a service as a means of circumventing an effective technological measure." Potential problems include (1) ambiguity of the term "effective technological measure" (*e.g.,* if a DRM vendor uses a cryptosystem that it knows is breakable,

is someone who breaks it "circumventing an effective technological measure"?), which is a problem with the DMCA as well, (2) lack of exceptions of the sort that the DMCA makes (*e.g.*, the encryption-research exception), (3) emphasis on US-style anti-circumvention rules without emphasis on a US-style fair-use doctrine, and (4) the need for major new legislation in many countries that may want to be parties to ACTA.

Question 4

(a) FNASRs are the rights to publish and reproduce the first North American print edition of a work. They are the publication rights that are most commonly sold in the US, and they are generally regarded as the most valuable publication rights.

(b) Authors may wish to make drafts of their works available online in order to get feedback before trying to sell the finished work to a publisher; however, publishers often refuse to purchase FNASRs from such authors, because they deem the work to have been made "publicly available." The legal question of whether a work that has been "leaked" online without the author's permission should be considered publicly available has not been resolved.

Question 5

(a) Using `robots.txt` files, website operators can instruct search engines' crawlers, in machine-readable form, not to crawl and index certain pages on the site. Despite the lack of an enforcement mechanism, reputable search engines comply with `robots.txt` instructions. Thus, people can put sensitive data into web pages, send the URLs of those pages to others who have a need to access those data, but not have those pages indexed by search engines and easily accessible by the world at large.

(b) "Contextualization" technology allows the subjects of online data objects, such as photos, videos, and articles, to annotate those objects with information that they think helps to frame and explain the way in which they are portrayed therein. Readers and viewers would be presented with the annotations at the same time that they are presented with the original (controversial) photos, videos, and articles. Contextualization could help level the playing field on which some parties disseminate "out-of-context" or simply false statements, and others try to clarify or refute them but currently cannot do so quickly enough to be effective.

(c) In his book "On Rumors," Sunstein has proposed "a general right to demand retraction after a clear demonstration that a statement is both false and damaging." Moreover, he has proposed that websites be required to take down false postings after receiving notice that they are false. This would be similar to the DMCA's "notice-and-take-down" provisions, under which websites are required to take down copyright material after receiving notice that it has been posted without the permission of the rights holder.

Question 6

(a) Notice/Awareness
Choice/Consent
Access/Participation
Integrity/Security
Enforcement/Redress

(b) Both "Notice/Awareness" and "Choice/Consent" are quite problematic in social networking. Evidence of this fact is provided every time there is a public outcry about a change in the way that Facebook handles users' "privacy preferences." People not only reveal that they are uncomfortable about the proposed changes (some of which are subsequently abandoned or changed further) but also make clear that they do not understand the extent to which Facebook already mines personal data and uses it to sell ads. This problem would be at least partially solved if social-networking sites effectively disclosed their data-collection policies, made more of their data collection opt-in instead of opt-out, and gave users meaningful choice. Currently, users are bombarded with an array of confusing options about which other users (friends, family, everyone, *etc.*) can view the photos, videos, and other stuff that they provide explicitly, but they must read the legalistic fine print of a "privacy policy" if they want to know the extent to which advertisers will be given information about them that they provide implicitly simply by using the site. Suppose instead that new users were told in simple language that they can either (1) use the service "for free" if they consent to advertisers' having access to the type of behavioral data that supports effective ad targeting or (2) pay a small monthly fee to use the service and not have behavioral data revealed to advertisers (and thus still be exposed to generic, "untargeted" ads but not have to worry about what else might be done with their data if they falls into the wrong hands). Then sites could still fulfill their social-networking missions by allowing users to share sensitive data with each other, but they would not mislead their users into sharing sensitive data with third parties without having explicitly consented to do so.

(c) Both "Notice/Awareness" and "Enforcement/Redress" are problematic in the context of academic records. Many students, parents of students, faculty members, and other employees of universities and colleges are ignorant of the existence of FERPA. This problem would be solved if universities and colleges distributed short FAQ sheets (***not*** pages and pages of legalese that no one would read) about FERPA to all interested parties. With respect to enforcement, the Department of Education's choices about how to respond to a FERPA violation (to request compliance or to cut off all federal funding) are completely inadequate and unrealistic, and individuals whose FERPA rights have been violated have no private right of action. To address at least the first part of this problem, the DoE could institute reasonable, credible penalties for FERPA violations, both light penalties for small-scale violations and heavier penalties (but not as heavy as a complete cut-off of funding, which is essentially a death penalty) for larger-scale violations. Moreover, it could actively investigate complaints, penalize violators promptly, and *publicize* the fact that it is doing so. Publicity of this sort would raise awareness of FERPA and perhaps deter violations.