Comment from: Adrian Tymes

Since you probably have many notes to read through, I shall attempt to keep this as brief as possible while adequately stating my contribution.

1. While there are access control mechanisms, the key here is "effectively". While the normal use that content providers envision may preclude such tactics as opening an ASCII file on a CD rather than use the reader that the provider supplies, which requires a key obtained for some non-zero price for each file read, such is in no way "effective" control. The only known way to prevent such access is to encrypt the content - and with the anti-cryptography legal environment promoted by law enforcement agencies, which is likely to be present for at least the next three years, encrypted files at any strength significant enough to remain "effective" are illegal to export. Given a choice between effective control and world wide markets, businesses will almost always choose the latter, but this means that their choice precludes controls that are not easy to break. (Note that reverse engineering remains legal in other countries; thus, no matter what legal controls exist in American territory, it would be a simple matter to set up a content breaking service in some other country for the benefit of Americans. Merely transmitting a controlled or uncontrolled file is not by itself illegal; the otherwise-illegal act of breaking the controls can be done where it is legal, perhaps even by a computer program without the owner of that program knowing of each specific incident - and the program itself certainly can not be held liable for breaking any laws.)

2. The technological measures that have historically been implemented to control content tend to shut out all derivative uses of the software - both negative uses such as plagarism and intellectual property theft, and allowable uses such as parody, political comment, and reviews. In the eyes of those who manage the companies that make these products, all of these uses are one and the same; in their opinion, there is no "allowable" use that does not feed their bottom line, therefore they encode their content such as to disallow all derivative use. Those measures that do not meet these criteria tend not to get used. Therefore I reccomend that the Librarian declare all classes of works, without exception, exempt from the anticircumvention provisions.

3. Negatively, almost without exception. Businesses find a way to sell their goods first; while much is made about piracy, it is telling that the sole anti-piracy measure employed by the majority of software products today is simply to trust that the consumer will not pirate.

Where more stringent access controls are in force, the market has reacted negatively relative to similar products which do not have any access control. Indeed, some e-commerce companies today are touting as part of their value the ability to help businesses that are consumers of products to avoid accidental piracy; there would be no value for said e-commerce companies if consumers wanted to pirate to the point that access control actually helped sales.

4. Not that I am aware of. Once people start selling a particular class of work, some people will continue to sell it no matter how much certain other people get ripped off. Indeed, certain business models - for example, shareware - are based on the premise of giving away the works for free and asking, but never forcing, the user to pay. These business models are sound enough that many companies profit from using them today.

5. See 4.

6. Fully. To take just one specific example: many years ago, a game by the name of "X-COM: UFO Defense" was released, with copy protection that required one to enter a code from the manual. While it did sell some copies, it was not exactly a smash hit and was discontinued. Years later, its copyright holders re-released it as a "classic"; the only things that changed were that the copyright protection was removed, the game now shipped on CD rather than multiple floppy disks, the manual is now a PDF on that CD rather than a separate printed volume, and the game is a bit cheaper. Sales have been good enough that, last I checked, the game is still for sale. While there are many factors that could account for this (better/cheaper ability to warehouse copies and fill demand, a market for classic games, more sales from lower cost), the lack of copy protection seems the only factor significant enough to account for this. This game is typical of cases of this nature that I have seen.

7. High-production-value movies and other interactive media. People wish to protect their wares when they invest a lot into them. While this is an understandable motive, the data suggests that the only effective technological form of piracy disuasion is one that is not quite access control: put the content into a single, undecompressable file that would take significant resources to move around. This in no way counts as access control, for once one has the file, one can access it freely; it just makes piracy uneconomical to the point where it is cheaper to buy the legitimate goods. The more access control is put on, the worse the product sells as the would-be legitimate consumers grow

more and more frustrated authenticating themselves.

8. Absolutely. Any work for which a time-based access control is imposed usually can not be effectively archived, for once the time is up, the archive becomes useless too. There are also access controls based on hardware identifiers; if new hardware is brought in to replace broken hardware, these universally reject their old authorizations because the new hardware has a new identifier. This applies across all works and classes of content that have been put into electronic form.

9. See 8.

10. Technological access controls do not care to what use that which they control will be put; that is purely a concern of those who sell the content. Those businesses that do not care to provide discounts to nonprofit educational groups, either because they believe themselves too small to afford such, because they do not believe (correctly or not) that a significant number of such groups would want to use their content, or simply because they have not thought of it, price their software the same both to rich companies and to (usually) poor nonprofits.

11. Cases could be made for any number of exceptions. Artistic and cultural uses, for example, could also be exempted. But only a finite number of these will be thought of. It would be better to exempt all uses equally, so as to cover all uses that one might want to exempt even if one does not think of them. Besides, these definitions can lend themselves to vagueness; one person's "education" is another person's "vocational training", and one person's class project can quickly become another person's multimillion dollar business without significantly changing its nature (case in point: Yahoo's early years).

12. Negative, where it has had any impact. For example, it is common practice among providers of "Web filters", which claim to block sites that contain pornography and other things unsuitable for minors, to also block any sites with negative reviews of their products, thus preventing users of their products from seeing these negative reviews. (They also commonly block troves of serious literary, artistic, and political sites; for example, sites which put up the full text of the Bible are sometimes blocked due in part to the Bible's occasional references to sexual activity. See http://www.peacefire.org/ for more details.) These products attempt to block access to the list of sites they ban, in order to interfere with reporting on the accuracy of those lists.

Similarly, it is in the competitive interest of most content providers to prevent giving away details of how their content works so as to avoid competition, but they make no distinction between commercial and noncommercial education about their products; the example of "Web filters" thus applies to varying degrees to all classes of works in electronic form.

13. Again, from the point of view of the businesses providing content, there is no "fair use" of their product which does not give them profit, legal issues aside. Businesses tend not to care about exemptions provided by the law in these cases, for the ones who would benefit from these exemptions typically do not have the resources to bring the law into play on their side; indeed, those who would commit "fair use" can often be driven into bankruptcy by a few frivolous lawsuits with barely enough legitimacy not to be thrown out of court. It thus becomes irrelevant what the law says in these cases.

14. See 12.

15. See 10 and 13. It is not a matter of "noninfringing" use, it is a matter of "nonprofitable" use: if a use does not profit the provider, then it is not allowed if the provider cares to say anything about it; this extends to reporting and education about the product, learning what algorithms the product uses so as to come up with something better, and so forth.

16. See 13 for why this is mostly a moot issue. Besides, any of these uses could easily be termed "fostering competition", which is not a protected use. I reccomend against estabilishing these classifications, as opposed to exempting all uses.

17. See 13. Technological measures tend to be blind to the specific application they are preventing; thus, for example, in preventing blatant stealing of a movie, an access control scheme that only allows a movie to be played a certain number of times would also (but "innocently") prevent frame-by-frame analysis of certain camera techniques by a film student. Exempting some uses grants license to ban others, with allowances for "accidental" or "unaviodable" banning of the protected uses; exempting all uses grants no such license.

18. This goes to the definition of "effective". An "effective" access control scheme is, by definition, one that can not easily be circumvented. As metioned back in 1, though, "effective" schemes are

not widely used. Ineffective schemes are widely used and widely broken; the recent lawsuit over DeCSS (a widely distributed piece of code that breaks the weak CSS access control scheme on DVDs, in order to allow DVDs to be used on operating systems without licensed DVD players, for example Linux) is merely a well publicized incident of how widespread these cracks are. (Search most of the larger public Web search engines, for instance MetaCrawler, for keyword "warez" for a graphic demonstration of how easy it is to find cracked software if one seriously wishes to find it. Also note that software without access controls tend not to get cracked and distributed in this manner.)

19. It has forced software to be priced closer to what the market will bear. Overpriced software gets cracked more frequently, for it is relatively more economical to crack it versus buying it. (Note that high priced software which actually provides high value, for instance professional CAD programs, tend not to get cracked as much as merely overpriced software.) This is a direct benefit to consumers.

20. While some producers of high production value content have been reluctant to embrace formats without much access control, the ease of copying of certain formats has encouraged lower production value content, with the standard distribution of high quality to low quality content. However, this same ease has also allowed easier searching of said content and searching for reviews of said content, making it easier for consumers to pick out the gems.

21. Many works have been promoted in easy-to-copy formats, with the express intent that the promotions be distributed. This is probably the most significant marketing impact.

22. Movies and other forms of art have been more impacted than productivity software. One possible cause is the lack of corporate cohesion among, say, the larger book writers and software publishers as opposed to the RIIA and MPAA for, respectively, music and movies: the latter act more like a monopoly as opposed to a bunch of competing interests, and thus have been less willing to make use of any competitive advantages in the new formats.

23. None. All "classes" should be exempt.

24. Yes; such has been identified (at least in my answers) in the answer to the specific questions.

25. Yes, as explained in 1 and 3.

26. No, as explained in 2 and 13.

27. I have stated my main points in my answers above. However, please keep in mind the practical effects of these rules, as well as the idealistic and legal effects. Technology pays far more attention to what is possible and economical than to what is legal. For example, if some activity is highly economical but technically illegal, especially if the law in that case practically never gets enforced (for example if it is impossible to enforce), then it will likely happen. The main effect that laws can have on this is to alter the economics of the situation, as well as - in certain cases - to send clear messages as to what is off limits.

28. None at this time.

29. I would not object if asked to testify, although I suspect I would need assistance in making the journey (unless I could testify by phone, teleconference, or some other way that would allow me to stay within, say, 100 miles of my home while testifying). I also suspect I might not have more to contribute than the above, though I am open to providing more information on any of these points - preferably with warning regarding what I will be asked, so I can research more supporting facts which doubtless will be desired.