

**Legal Aspects of Electronic Record Retention:
Playing Safe in an Era of New Options**

**Presented on April 4, 2005 at the Spring 2005 meeting of
The Association of Specialized and Professional Accreditors (ASPA)
Lucien Capone III
University Counsel
The University of North Carolina at Greensboro**

INTRODUCTION

I believe that historians will view the “electronic revolution,” which took root in the last half of the 20th century, to be just as significant to the course of human history as was the “industrial revolution.” Ironically, recorded history itself is being kept more and more frequently only in electronic format. Accreditation, which at its heart is an information gathering process, is no exception to that trend.¹ An increasing number of educational programs are putting all or parts of their self-study on-line. Laptops are no longer considered site team luxuries, but have become an absolute necessity. Executive directors, whose offices have become cramped obstacle courses of boxed self-studies, site team reports, board member materials, etc., must increasingly turn to digitized storage as the only affordable alternative to converting expensive office property into warehouse space.

Although rosy predictions of “paperless offices” were overblown, there can be no dispute that unimaginably vast amounts of information now exist only in the form of magnetically or optically sequenced atomic particles stored on silicon chips, magnetic tapes, CDs, DVDs and other electronic devices. This quantum leap in information storage technology (akin to the invention of the printing press) has been, at the same time, a blessing and a curse; a blessing because it allows for storage of massive quantities of data in a very, very small space; a curse because it allows us all to indulge our tendencies towards laziness, as pack rats, procrastinators, or all three. As one federal judge recently lamented, “Information is retained not because it is expected to be used, but because there is no compelling reason to discard it.”²

One result of this digital warehousing phenomenon is that “electronic archaeology” is fast becoming a multi-billion dollar industry.³ From a defense lawyer’s standpoint, “TMI” (too much information) can be hazardous to your legal and financial health. Plaintiffs’ attorneys have become experts at data mining. (Do you really want a bunch of lawyers rummaging around in your electronic attic?) That is one reason defense lawyers (like me) tend to be zealous advocates of tightly written records management policies. As I said in a previous paper presented at ASPA’s fall 2003 meeting, “the best protection is to have a comprehensive records retention policy that puts realistic time limits on the length of time that records are kept.”⁴

*This paper was provided by ASPA to attendees of the Spring 2005 ASPA meeting and posted to the ASPA web site with the permission of the author.

Another concern, information security, is not a new consideration, but the digital environment presents new challenges for maintaining the security and integrity of sensitive data. Accreditors come into possession of confidential information throughout their work. Student and personnel records, personally identifiable health information (or “PHI” in HIPAA parlance), proprietary data, and just down-right potentially embarrassing material populate accreditation files. Much of this material is transmitted as well as stored, electronically. Guarding against accidental loss or theft of that information is of paramount importance. To compound the problem, there is increasing pressure from Congress and CHEA to make more of this information a matter of public record in the belief that it will foster greater accountability.⁵

Additionally, digitizing materials authored by others necessitates consideration of the federal Copyright Act. In my experience, few people truly understand the legal implications of making, storing and using digital copies. There are many misconceptions about what it takes to obtain a copyright and about the concept of “fair use.”

This paper will explore the statutory, regulatory and court-made requirements affecting electronic record retention and the implications of those requirements for policy writing. This paper will also touch on copyright concerns and will suggest strategies for dealing with it efficiently.

THE LEGAL UNDERPINNINGS OF ELECTRONIC RECORDS RETENTION

A. Definition

Although the law has yet to reach definitional consensus on the term “electronic record,” most definitions are quite broad and written in such a way that they will encompass new and unforeseen technologies. A prime example, and as good a definition as any, can be found in the Uniform Electronic Transactions Act (UETA) which defines the term to mean any “record created, generated, sent, communicated, received, or stored by electronic means.” The word “electronic” means technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.⁶

As a general rule, most laws governing records retention either expressly list “electronic records” as one variety of record that must be kept or simply state that covered records include all those documents fitting the subject matter of the law regardless of format. An example of the former is the federal Freedom of Information Act (5 U.S.C. § 552(f)(2)) that defines “record” to include “any information . . . maintained by an agency in any format, including an electronic format.” An example of the latter is the North Carolina Personnel Records Act⁷ which defines a personnel record to include any record relating to a person’s employment by the State “in whatever form or wherever located.” The key point here is that unless a statute or regulation expressly limits the definition of “records,” you must assume that electronic records are covered.

B. Statutes and Regulations Applicable to Accreditation Records

The most obvious records retention requirements affecting accrediting bodies are those found in sections 602.15 and 602.23 of the U.S. Department of Education's regulations governing recognition of accrediting agencies.⁸

Section 602.15 requires that the accrediting body maintain "complete and accurate" records of:

- (1) Its last two full accreditation or preaccreditation reviews of each institution or program, including on-site evaluation team reports, the institution's or program's responses to on-site reports, periodic review reports, any reports of special reviews conducted by the agency between regular reviews, and a copy of the institution's or program's most recent self-study; and
- (2) All decisions regarding the accreditation and preaccreditation of any institution or program, including all correspondence that is significantly related to those decisions.

Section 602.23 requires the agency to maintain and make available to the public, upon request, written materials describing:

- (1) Each type of accreditation and preaccreditation it grants;
- (2) The procedures that institutions or programs must follow in applying for accreditation or preaccreditation;
- (3) The standards and procedures it uses to determine whether to grant, reaffirm, reinstate, restrict, deny, revoke, terminate, or take any other action related to each type of accreditation and preaccreditation that the agency grants;
- (4) The institutions and programs that the agency currently accredits or preaccredits and, for each institution and program, the year the agency will next review or reconsider it for accreditation or preaccreditation; and
- (5) The names, academic and professional qualifications, and relevant employment and organizational affiliations of:
 - (i) The members of the agency's policy and decision-making bodies;
 - (ii) The agency's principal administrative staff.

While neither of these regulations mentions electronic records per se, one must assume that the format in which these records are kept is irrelevant to the requirement, i.e., electronic records relating to the subject matter are covered.

I should also note that these regulations establish the minimum amount of information that must be kept in order to maintain recognition status. Any documentation that establishes compliance with other Department of Education recognition requirements should also be kept. For example, Section 602.21 requires that standards be periodically reviewed and that the accrediting body's constituencies be given an opportunity for input. Unless you retain documentation of your standards review process, I think it will be difficult to establish your compliance with this mandate.

In addition to documents that relate directly to accreditation functions, most accrediting bodies or their parent associations keep employment and payroll records, financial data including tax returns, etc. Federal and state laws often establish record keeping requirements in those areas as well. For example, the Fair Labor Standards Act requires that payroll records be kept for three years.⁹ So, these records of your day-to-day operations must be factored into the records retention mix as well.

C. How Long Should Electronic Records be Kept?

The short, (defense lawyer's) answer to the question of how long electronic records should be kept is "only for so long as the law requires or for as long as you actually have use for them, and not a moment longer." There is no bright line number.¹⁰ In typical lawyerly fashion, my real answer is that "it depends."

Any records management program must ensure that legally required documents are kept for at least the minimum prescribed time periods. But, are there circumstances under which they should be kept for a longer period of time? In my view there are two answers to that question. First, there may be records you think are critical to preserving historical continuity, for example, minutes of strategic planning meetings or of policy development sessions. Board members come and go, and these records may help their successors understand the intent behind certain policies and standards, hopefully preventing repetitive "wheel inventing" exercises. More importantly, they may help prevent inconsistent decision making. These calls are tough to make, but the executive director is the person most likely to have the long-term perspective or "corporate memory" needed to make that decision.

The second reason may be litigation or governmental investigations and enforcement actions. As I will discuss next, these latter circumstances will almost always trump your retention and disposition schedule.

RETENTION OF ELECTRONIC RECORDS IN THE FACE OF LITIGATION OR GOVERNMENT ENFORCEMENT ACTIONS

A. "Spoliation" (be afraid, be VERY afraid)

Electronic records present certain unique factors that have only recently been addressed by the courts in the context of formal "discovery" proceedings. For those of you fortunate enough to have avoided litigation, "discovery" is the pre-trial process where both sides find out as much as they can about what cards their opponent is holding. Trial by ambush is no longer tolerated by the courts. The tools of discovery include depositions, interrogatories, requests for admission, subpoenas (including subpoenas *duces tecum*) and requests for production of documents. The later two devices, the subpoena *duces tecum* and request for production, are the ones most likely to require you to turn over your electronic files. The only real difference between the two is that the

request for production goes to persons or entities named in the lawsuit, while subpoenas are issued to non-parties who may hold evidence relevant to the parties' case.

E-mail, instant messaging logs, and backup tapes have become favorite targets for plaintiffs' lawyers during discovery because they often prove to harbor the proverbial "smoking gun." It is an unfortunate fact that people tend to say things in an e-mail that they would never, ever consider putting into a letter or memo.

When litigation is filed or, for that matter, even threatened, or if you receive notice that government officials want to audit your records, there is an affirmative legal duty to preserve all records having anything to do with the subject matter, regardless of your disposition schedule. Failure to do so can have dire consequences. The term "spoliation" should strike fear into the heart of any records manager for "there be dragons!" Spoliation is the destruction or loss of documentary evidence, whether it occurs through negligence, recklessness or intentional acts. Other than outright perjury, I have never seen anything anger a judge more than the revelation that one party to litigation "lost" records demanded by the other side through the formal discovery process. When spoliation occurs in criminal investigations people go to jail, as happened when employees of Arthur Andersen destroyed documents related to their audits of ENRON.¹¹ When spoliation occurs in civil cases, both companies and individuals get held in contempt of court and fined. This is exactly what happened in *Massachusetts School of Law at Andover, Inc. v. American Bar Ass'n*, where the court found that the law school's attorney had not acted in good faith when responding to discovery requests and court orders. In a very colorful statement slamming the school's attorney, the judge said, "It is not 'good faith' for a lawyer to frustrate discovery requests and court orders with successive objections like a magician pulling another and another and then still another rabbit out of the hat; . . . discovery is not poker where cards are turned up one at a time."¹² He then ordered the lawyer to personally pay several thousand dollars in contempt of court fines.

B. Zubulake v. UBS Warburg (thrills and chills)

In July of 2004, a federal judge in New York sent thrills throughout the plaintiffs' attorney community, and chills throughout the defense lawyer ranks, when she wrote a blistering opinion criticizing UBS Warburg and its in-house counsel for failing to personally prevent the destruction of employee e-mails.¹³ In that case, Judge Shira A. Scheindlin found that UBS Warburg had notice that the plaintiff, Laura Zubulake, was contemplating legal action for gender discrimination as early as April 2001 because of comments she made about filing a charge with the Equal Employment Opportunity Commission. Judge Scheindlin held that the duty to preserve relevant evidence attached *at that time* because litigation was (or should have been) "reasonably anticipated." Even though UBS Warburg's in-house attorneys issued a missive in August of 2001 instructing employees not to destroy electronic and hard copy records, nothing was said about backup tapes. When Zubulake's lawyers later asked for e-mails stored on backup tapes it was discovered that the tapes had been routinely recycled. When the matter was brought to the judge's attention, her Honor faulted the company, and its lawyers, for having failed

to both locate *and monitor* compliance with the litigation hold throughout the pendency of the lawsuit. Judge Scheindlin went on to find that UBS Warburg employees also continued to destroy e-mails in the face of their own lawyer's directives. Based on the joint failures of UBS Warburg and its counsel, her Honor imposed sanctions ranging from monetary fines to the dreaded "adverse inference" jury instruction, where the jury is told they may infer that UBS Warburg was intentionally destroying evidence that would have helped Ms. Zubulake prove her case.

C. When is a Backup not a "Backup?"

Backup tapes are veritable gold mines of undiscovered information. But extracting that data can be quite difficult and hugely expensive. Who has to bear that burden if you get sued and the plaintiff's lawyer asks for it? Right...YOU do! Under the discovery rules, the presumption is that the responding party must bear the expense of complying with discovery requests.¹⁴ Further, "if a party chooses an electronic storage method, the necessity for a retrieval program or method is an ordinary and foreseeable risk."¹⁵ As one judge pointed out, "Too often, discovery is not just about uncovering the truth, but also about how much of the truth the parties can afford to disinter...discovery expenses frequently escalate when information is stored in electronic form."¹⁶ But, there is some light at the end of this seemingly endless fiscal tunnel. Because of the huge expense required to dig information out of backup tapes, the courts have been willing to carve out an exception for backups that are used purely for disaster recovery rather than those that are actively used for information retrieval.

Backup tapes, [created for the event of disaster recovery] are not archives from which documents may easily be retrieved. The data on a backup tape are not organized for retrieval of individual documents or files, but for wholesale, emergency uploading onto a computer system. Therefore, the organization of the data mirrors the computer's structure, not the human records management structure...¹⁷

A party that happens to retain vestigial data for no current business purposes, but only in case of an emergency or simply because it has neglected to discard it, should not be put to the expense of producing it. On the other hand, a party that expects to be able to access information for business purposes will be obligated to produce that same information in discovery.

A caveat is required here. Not everyone agrees that disaster recovery backups should be exempt. Some courts hold that if a plaintiffs' attorney demands them, you will have to produce them. However, in that case the cost of extracting information might be shifted away from you and to the plaintiffs.

D. Other Considerations

The spoliation issue is just one side of the coin. On the flip side lies the need to keep documents that will help you prove your side of the case, e.g., that your Board's decision to deny or revoke a program's accreditation was based on sound professional judgment rather than on irrelevant factors or that the decision was not "arbitrary and capricious." The key legal consideration regarding length of time to retain such records hinges on whatever statute of limitations applies. Unfortunately, every state sets its own limitations periods and, even within a state, different periods are set for different types of lawsuits. Generally speaking, the most usual time period is three years from the date of the alleged wrongful act or decision. I advise my clients to keep relevant records for one to two years beyond the limitations period because various things can "toll" the running of that period. Having said that, I strongly advise you to consult your legal counsel.

Finally, the format in which you keep electronic records should also be carefully considered. If you kept records on 8-track tapes, or microfilm, it is probably getting harder to retrieve that information easily and cheaply. I have documents I created years ago in Macintosh's word processing jewel called "Clarisworks" that are totally irretrievable using Word, WordPerfect, or any other software I've been able to find, now that I've been forced by evil IT snobs to migrate to the Windows environment at my workplace. So, my word to the wise here is that you shouldn't go with the latest fad in technology, but wait until it becomes established, and then upgrade.

LEGAL REQUIREMENTS REGARDING INFORMATION SECURITY AND INTEGRITY

Accreditors have always understood the need to protect confidential information. It is a hallmark of the trust relationship we establish with our institutions and programs. When all of this information was on paper, security was a simple matter of ensuring that file cabinets and doorways were kept locked. Digital storage also requires locks and keys. First, any room where the server or other storage medium is housed must have physical safeguards against unauthorized entry. Computer theft is at an all time high. But electronic storage and transmission adds a new dimension to the security issue. Technical safeguards such as passwords, encryption, and automatic logoff must be implemented to ensure that confidential data is not accidentally transmitted to or viewed by the wrong person, and to ensure (as much as possible) against hacking. The more sensitive the data, the higher the legal standard will be.

A prime example is the Health Insurance Portability and Accountability Act (HIPAA) and its implementing regulations.¹⁸ HIPAA requires that covered entities "ensure" that an individual's personally identifiable health information (PHI), be kept private. The word "ensure" always gets a lawyer's attention because it is the highest legal standard of care that can be imposed short of strict liability. It means that the keeper of this PHI must take every prudent and reasonable step necessary to secure the data against all known or reasonably foreseeable losses. Accreditors of health care providers are specifically mentioned in HIPAA and are classified as "business associates" of those entities.¹⁹ As

such, accreditors also have a legal obligation to meet HIPAA's privacy and security requirements.²⁰

Similarly, Department of Education regulations implementing the Federal Education Records Privacy Act expressly mention accreditors as being authorized to obtain student files without first obtaining the student's written consent.²¹ Here again, accreditors are bound by that law to maintain the confidentiality of those records.

COPYRIGHT LAW AND ELECTRONIC RECORDS

When you receive documents that you did not create, you must assume that those documents are protected by copyright. What most people (including a lot of lawyers) don't know is that since 1989, when the United States became a party to the Berne convention, a work becomes automatically copyrighted as soon as the work is "fixed in a tangible medium." There is no need to register the work with the copyright office in the Library of Congress unless and until the copyright owner intends to actually sue somebody for infringement. There is also no need to affix the copyright symbol, ©, or any other notation of the owner's copyright claim. A work can become "fixed in a tangible medium" in any number of ways including on paper, a photograph, on video or audio tape, on a CD ROM or DVD, or even in a computer's hard drive. Therefore, if you can perceive the work in some form other than a purely live performance, the odds are excellent that it is protected by copyright, unless there is an express disclaimer given by the author or copyright owner.

It is equally important to note that some information may not be copyrighted at all. The prime example is factual data (e.g., the number of students in attendance at an institution or program). However, if that data is arranged in some unique format the document (but not the data itself) may well be covered.

The Copyright Act reserves to the copyright owner (who is usually, but not always the author) the exclusive right to make copies, to distribute by sale, loan, or gift, to make derivatives (e.g., modifications), to perform and to display the work. The owner can dispose of any or all of those rights. The most usual way this is done is through a license which is simply legal permission to use the work. The only exception to the owner's grant of exclusivity is "fair use." Fair use is a complicated topic whose detail is beyond the scope of this paper.²² However, in a nutshell, fair use applies when the use (without license) is done for commentary, news reporting, parody, classroom, scholarship or research purposes AND the use for those purposes can be considered "fair" when analyzed using the following four factors:

(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; (is it more fact than fiction, is it published or unpublished?)

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

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

Of these four factors, (3) and (4) seem to get the most emphasis by the Courts, especially the market impact factor. Fair use is an “affirmative” defense meaning that the person claiming it has the burden of proving it.

So, let’s look at how this applies to you as an accreditor.

When you receive self-study materials, either in hard copy or by mail, there is probably a great deal of copyright protected material included, separate and apart from “just the facts.” For example, the materials may include photographs, articles, institutional promotional and catalog materials, etc. If you make additional copies of those materials or if you make a digital copy you are, at least technically, usurping the owner’s exclusive rights. Fortunately, the courts recognize that there is an implied license to use copyright protected materials under certain circumstances. An implied license will arise where “(1) a person (the licensee) requests the creation of a work, (2) the creator (the licensor) makes the particular work and delivers it to the licensee who requested it, and (3) the licensor intends that the licensee copy and distribute his work.”²³

Applying these principles to self-study materials, one can see that anything in the materials that was created *for the purpose* of the self-study will be subject to an implied license to copy and distribute those materials as necessary to carry out the accreditation function. But there are two important caveats here. First, the self-study is often a collection of materials, some of which were created for the purpose of the self-study and some that were created for an entirely different purpose, but have been submitted to document compliance with the accreditor’s standards. This latter category is the most problematic because the institution itself may not actually own the copyright to those previously created materials. For example, if a faculty member’s journal article is included, in all likelihood the faculty member or his or her publisher may actually own the copyright to that work.²⁴ Therefore, it is important that the accrediting body obtain some assurance from the program that it has permission (i.e., a license) to use that work in the self-study.

My advice would be that the accrediting body obtain a certification from the program chair that all materials included in the self-study are submitted with permission of any and all copyright owners. Otherwise, the accrediting body may have to resort to a fair use argument if challenged. In my opinion, the courts will sustain a fair use defense, because it is unlikely that the few copies you make for your Board members will have much impact on the market for the original, and because you are using it for nonprofit, educational purposes. But you need to be aware that there is a risk here and you should consult your own legal counsel. Also, do not post those materials to a website unless that site is password protected. Otherwise, you’ve just given the whole world access to the copyrighted materials and you may well have destroyed the copyright owner’s market.

The second (and related) caveat here is that the accrediting body must limit its use of the self-study materials to traditionally accepted forms of copying and dissemination used in the accreditation field. In *New York Times, Inc. v. Tasini*,²⁵ the United States Supreme Court held that the newspaper violated freelance authors' copyright when it reproduced their articles in an electronic database. The Court found that such a use had not been contemplated or agreed to by the authors and exceed the paper's license whether express or implied.

CONCLUSION

Although the advent of electronic records has facilitated storage and access to vast amounts of information, thereby increasing efficiencies and reducing costs, there are a plethora of legal concerns that must be addressed. My purpose in this paper is not to resolve all of those concerns, but simply to raise awareness and to provide a warning that one may not blithely assume that creating and maintaining electronic records is "no big deal" or no different than creating and maintaining hard copy files. This is an area that requires consultation with persons having technical expertise in digital data management. I also strongly encourage you to have your attorney review your records management policy, and to consult with him or her as soon as you receive any threat of litigation.

Endnotes

¹ Obermeir, T, *Using the Internet for an Accreditation Self-Study Portfolio*, Journal of Industrial Technology, Vol. 21, Number 1 (Jan through March 2005), retrieved, February 22, 2005 from, <http://www.utsystem.edu/ogc/intellectualproperty/copypol2.htm>.

² Rowe Entertainment, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 423 (S.D.N.Y. 2002).

³ Vaughan, J. *Data mining comes of age*, ADTmag.com (May 1, 2002) retrieved from <http://www.adtmag.com/article.asp?id=6286> on February 22, 2005.

⁴ Capone, L. (2003, September), *What, Me Worry?: An Overview of Legal Concerns for Accreditors*, retrieved February 22, 2005 from <http://www.aspa-usa.org/resources/capone.html>.

⁵ Proposed amendments to the Higher Education Act, if enacted into law, will require publication of any award of accreditation, *including findings*, any adverse accreditation action taken with respect to an institution together with the institution's comments, a list of site team members' by name, agency affiliation and professional experience, the agency's process of selection, training and evaluation of site teams)and the agency's code of conduct. HR 507, 495(a)(8), 109th Cong. (2005). Additionally, perhaps in an effort to head off Congressional action, CHEA is proposing revisions to its recognition standards that will require accrediting bodies to adopt standards mandating that institutions and programs, in consultation with the accrediting organizations, inform the public of all accreditation decisions on accreditation status and the reasons for these decisions." CHEA, Recognition of Accrediting Organizations Policies and Procedures, draft 1, (March 22, 2004).

⁶ Uniform Electronic Transactions Act § 2.(5), (7)(1999).

⁷ N.C.Gen.Stat. § 126-22, et. seq.

⁸ 34 C.F.R. § 602.15, .23.

⁹ A convenient listing of many of these statutes can be found at:
http://www.whad.com/labor_library/Statutory_Recordkeeping_Requirements.htm.

¹⁰ There are several good articles on this subject. One example is Skupsky, D. *Establishing Retention Periods for Electronic Records* (2004), at:
<http://www.accutrac.com/Newsletter/Establishing%20Retention%20Periods%20for%20Electronic%20Records.pdf>. Additionally, The Council of State Historic Records Coordinators has a web page devoted to various state policies about management of emails. http://www.coshrc.org/arc/states/res_email.htm

¹¹ *Judge fines Arthur Andersen \$500,000*, Accountancy.com, Oct. 16, 2002, retrieved February 23, 2005 from: <http://www.accountancy.com.pk/newsprac.asp?newsid=20>.

¹² 914 F.Supp. 1172 (E.D.Pa. 1996).

¹³ *Zubulake v. Warburg*, 2004 WL 1620866 (S.D.N.Y. July 20, 2004).

¹⁴ *Oppenheimer Fund, Inc. v. Sanders*, 437 U.S. 340, 358, 98 S.Ct. 2380, 57 L.Ed.2d 253 (1978).

¹⁵ *In re Brand Name Prescription Drugs Antitrust Litigation*, Nos. 94 C 897, MDL 997, 1995 WL 360526 (N.D. Ill. June 15, 1995).

¹⁶ *Rowe Entertainment, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 423 (S.D.N.Y.2002).

¹⁷ Kenneth J. Withers, *Computer-Based Discovery in Federal Civil Litigation*, SF97 ALI-ABA 1079, 1085 (2001).

¹⁸ 45 C.F.R. § 164.501, et seq.

¹⁹ 45 C.F.R. § 164.502(e)(2).

²⁰ 45 C.F.R. § 164.531(j)(2).

²¹ 34 C.F.R. § 99.31(7).

²² More information about fair use, especially in academic settings, can be found on the University of Texas General Counsel's web site at: <http://www.utsystem.edu/ogc/intellectualproperty/copypol2.htm>

²³ *Atkins v. Fischer*, 331 F.3d 988, 992 (D.C. Cir. 2003).

²⁴ In the event of a legal challenge, courts will most likely treat the self-study as a “collective work” under the Copyright Act. 17 U.S.C. § 201(c). Copyright in each separate contribution to a collective work is distinct from copyright in the collective work as a whole, and vests initially in the author of the contribution. In the absence of an express transfer of the copyright or of any rights under it, the owner of copyright in the collective work is presumed to have acquired only the privilege of reproducing and distributing the contribution as part of that particular collective work, any revision of that collective work, and any later collective work in the same series.

²⁵ 533 U.S. 483, 121 S.Ct. 2381 (S.Ct. 2001).