

Chapter XVII

INFORMATION TECHNOLOGY AND CONSTRUCTION LAW

By: Ed Hood
Clark Hill, P.L.C.

who acknowledges and thanks Clark Hill summer associate Bryan H. Zair for his research and input that formed the basis for portions of this chapter.

17.1 Overview

“Every few hundred years in Western history there occurs a sharp transformation. We cross . . . a ‘divide’. Within a few short decades, society rearranges itself—its worldview; its basic values; its social and political structure; its arts; its key institutions. Fifty years later, there is a new world. And the people born then cannot even imagine the world in which their grandparents lived and into which their own parents were born.”

Peter Drucker, Post-Capitalist Society

Information technology is one of the forces that has “sharply transformed” our society over the past 50 years. It includes “the information that businesses create and use as well as a wide spectrum of increasingly convergent and linked technologies that process the information.”¹ Information technology has advanced at a remarkable pace. Moore’s Law, articulated by Intel co-founder Gordon Moore in 1965, states that computing power (expressed as the number of processors on a computer chip) doubles every 18-24 months.² Moore’s Law has continued unabated, and is expected to hold true at least through this decade.³

The direct implication of Moore’s Law is that computing has become progressively faster, cheaper, and easier. Indirectly, this steady advancement has afforded increasing opportunities for businesses to become more nimble, efficient, and competitive. These opportunities have been further catalyzed by the advent of the Internet, which has ushered in an era of prolific electronic communication. According to estimates by the Yankee Group, the average worker receives five times the number of e-mails as she does phone calls. In the same vein, the Radicati Group projects that, by 2004, 42 billion e-mail messages will be sent per day.⁴

So, what does information technology have to do with construction or construction law, considering that buildings are still erected with cement and steel, rather than bits and bytes? Plenty, it turns out. Just as advancements in engineering have brought substantial improvements in building technology, so too has information technology improved the business processes of construction firms. But information technology has its baggage, raising complicated business and legal issues.

17.2 Technology and Construction Practice

There are countless ways in which information technology has improved the productivity of construction firms and the manageability of projects. Some specific construction-related IT applications include: Company Web Sites: Company web sites are nearly as ubiquitous as phone book listings. Virtually every company now has a web site, with varying degrees of sophistication and functionality. For example, some companies prefer to use their web sites essentially as on-line brochures, while others contain interactive features that allow retrieval and uploading of information and resources. This distinction can have important jurisdictional consequences, as discussed below.

Project Web Sites: A project web site is a domain – often “hosted” by an independent application service provider (ASP) - where electronic files are stored, managed, and shared by authorized users. As part of the World Wide Web, such sites can be accessed by the general public, but specific portions of the site are restricted to authorized visitors. Proponents of project web sites boast that the sites allow project participants to collaborate on projects in real time, and consolidate resources such as bidding systems, construction management tools, news and information, building project catalogs, and other services. Project web sites have generated plenty of excitement, but many wonder whether they are all sizzle and no steak. Researchers at Purdue University are trying to determine just that. They are performing a survey relative to use of project management sites leased from ASPs, such as Buzzsaw by Autodesk, Constructw@re, ProjectTalk by Meridian Project Systems, Viecon.com, BuildOnline.com; Citadon and PrimeContract by Primavera.⁵ It remains to be seen whether this technology has been, or will soon be, fully embraced by large and small firms alike. Even if the technology itself is accepted, with notable exceptions many small trade contractors lack the resources to invest in hardware, software and broadband Internet access necessary to maximize use of a project web site.

Extranets: Extranets are company-hosted sites that are accessible only by authorized users. They are popular among design professionals. Informal empirical evidence suggests that extranets are more prevalent than project web sites, primarily because of security concerns, ease-of-use, and narrower functionality.

Electronic Bidding: Government agencies that procure high volumes of construction services through traditional design/bid/build processes are making greater use of electronic bidding. The Michigan Department of Transportation (MDOT) is on the leading edge of this application.⁶ MDOT has implemented an electronic bidding process whereby firms submit bids through a secure web site operated by an independent ASP. The ASP submits the bids to MDOT following the bid deadline. The process is touted as beneficial to bidders by eliminating submission costs and misunderstandings over illegible handwritten figures. The system also offers greater bidding flexibility. Prior to the bid deadline, bidders may change their bids through a password-protected page on the ASP bidding site. Meanwhile, MDOT stands to benefit from administrative efficiencies, reduced errors in transcribing paper bids to electronic files, and from speed in decision-making.⁷

Electronic Commerce: Commercial transactions are increasingly carried out through electronic means. The Uniform Electronic Transactions Act (“UETA”), adopted in Michigan and codified at MCL 450.831, et seq., reflects and legitimizes this trend. Under the UETA, parties are authorized, with certain exceptions,⁸ to contract using electronic documents and electronic signatures. The UETA provides that where parties expressly or impliedly agree to conduct a transaction by electronic means an electronic record satisfies a law requiring that the record be in writing, and an electronic signature satisfies legal signature requirements.⁹ The UETA further authorizes electronic record retention and provides that, in civil and criminal proceedings, evidence of a record or signature “shall not be excluded solely because it is in electronic form.”¹⁰

Data Storage and Retrieval: We are increasingly moving toward a paperless world. As a result, storage of electronic documents is far less expensive than hard-copy counterparts. As one court put it, electronic data has become voluminous because, unlike paper documents, “the costs of storage are virtually nil. Information is retained not because it is expected to be used, but because there is no compelling reason to discard it.” *Rowe Entertainment, Inc v William Morris Agency, Inc*, 205 FRD 421, 429 (SDNY 2002). As discussed below, however, even electronic data does not last forever – at least not in readily accessible form – leading to a multitude of issues pertaining to record retention and evidence preservation.

Procurement: Electronic procurement of many construction commodity items has become common. Vast numbers of high-volume construction materials suppliers have supplemented their traditional “bricks and mortar” business with internet retailing. Additionally, according to a recent *Engineering News Record* article, construction is the fastest growing segment for eBay.¹¹

17.3 Legal And Practical Implications Of Advancements In Information Technology

17.3.1 The Pitfalls of Off-The-Shelf Software

Dozens of software vendors now offer integrated project management software that can be purchased “off-the-shelf,” in a standard format. While there are clear cost advantages to purchasing standardized software, managers need to be cautious about how such programs are actually used. In other words, while customized software adapts to a firm’s business practices, with standardized software, the sequence is reversed, and business practices “often must be modified to fit the system.”¹²

The problem is when the business process is not modified to fit the software. For example, a standard computer-generated daily field report might contain a data field for “delay impacts.” If a user is not accustomed to completing such a field, or worse, checks off “0” in order to plough through the form, such entries (or lack thereof) could have a devastating impact on future claims. The moral is that, if a firm uses standard software, its conduct has to be shaped to conform to the format inherent in the software.

17.3.2 Discovery of E-Mail and Other Electronic Evidence

As noted above, e-mail has become the most prolific mode of business communication in the United States, far outpacing telephone and first class mail. E-mail is emblematic of how information technology progress has made business communication faster, cheaper, and easier to use. Precisely because e-mail is faster, cheaper, and easier to use than other means of communication, it is usually less formal and, at times, careless, in its presentation and content. This casualness is typically owing to a misguided belief that e-mail communication is private, or that once deleted, the communication disappears into the ether. Microsoft and countless other companies¹³ have learned the hard way that e-mail is not private, not made of disappearing ink, and can be exploited by one’s adversaries in litigation¹⁴

It is well-established that, in state and federal courts, e-mail and other electronic documents are discoverable. One federal court recently summed up the application of discovery rules to electronic data in this way:

As the Advisory Committee Notes to Rule 34, Federal Rules of Civil Procedure make clear, discovery of "documents" "applies to electronic data compilations from which information can be obtained only with the use of detection devices." Moreover, it is a well accepted proposition that deleted computer files, whether they be e-mails or otherwise, are discoverable. See, *Rowe Entertainment, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421, 427, 431 (S.D.N.Y. 2002) (stating that "electronic documents are no less subject to disclosure than paper records," and only questioning who should bear the cost of such discovery, especially for back-up tapes or deleted e-mails); *McPeck v. Ashcroft*, 202 F.R.D. 31, 31, 34 (D.D.C. 2001) (declaring that, "during discovery, the producing party has an obligation to search available electronic systems for information demanded," and ordering a limited back-up restoration of e-mails); *Kleiner v. Burns*, 2000 U.S. Dist. LEXIS 21850, 2000 WL 1909470 (D. Kan. December 15, 2000) (noting that Rule 26(a)(1)(B) requires description and categorization of computerized data, including deleted e-mails, and stating that "the disclosing party shall take reasonable steps to ensure that it discloses any back-up copies of files or archival tapes that will provide information about any "deleted" electronic data"); *Simon Property Group L.P. v. my Simon, Inc.*, 194 F.R.D. 639, 640 (N.D. Ill. 2000) ("First, computer records, including records that have been 'deleted,' are documents discoverable under Fed. R. Civ. P. 34."); *Playboy Enterprises v. Welles*, 60 F. Supp. 2d 1050, 1053 (S.D. Cal. 1999) ("Plaintiff needs to access the hard drive of Defendant's computer only because Defendant's actions in deleting those e-mails made it currently impossible to produce the information as a 'document.'").¹⁵

Given that e-mail and other electronic documents are clearly discoverable, what are the implications for contractors? First, a prudent company should notify all employees that e-mail is neither private nor temporary, that e-mail is stored in the company’s computer system and may be seen by persons other than the named recipients, and that they should prepare e-mail communications with the same care and decorum as hard copy correspondence or inter-office memoranda. Second, firms must implement both

document retention parameters that meet business needs and evidence preservation controls that ensure that evidence is not destroyed. Document retention policies are discussed below.

17.3.3 Electronic Document Retention Policies

Generally speaking, document retention is a two-dimensional issue, i.e., (1) how long should records be retained?; and (2) in what form should records be retained? As discussed below, there is no black-letter answer to either of these questions as they relate to electronic documents, and each company must make its own determination based on a number of factors.

17.3.3.1 Length of Retention

In the normal course of business (i.e., assuming there is no active litigation), how long a company should retain documents depends on the nature of its business, regulatory requirements, and the places where it conducts business. For example, the Federal Acquisition Regulations pertinent to federal projects require contractors to retain records, and to make them available for inspection for three years after final payment, or longer if the specific contract so requires.¹⁶ Beyond express requirements for records retention, firms may wish to retain records for longer periods. For example, a construction firm may determine that it should retain records for Michigan projects for at least six years, in light of the Michigan limitations period for breach of contract actions,¹⁷ and the statute of repose.¹⁸ Again, however, each firm must make its own determination based on applicable laws and contract requirements, and the nature of its business risks.

Courts require firms to modify retention practices in the event litigation is likely or has been commenced.¹⁹ After litigation has started, a party has a clear duty to preserve evidence that is relevant or likely to lead to the discovery of admissible evidence – even if the adversary has not yet expressly requested production of the information.²⁰ Moreover, while no bright-line rule has emerged, it is arguable that a firm has a duty to preserve electronic data once a dispute has become possible. For the construction firm, this duty could arise with the first disputed change order, differing site condition, or other event that might affect the relative obligations of parties to a construction project.

In Michigan and elsewhere, a party may be punished for the destruction of evidence which, when intentional, is known as “spoliation.” A finding of spoliation can lead to an assortment of undesirable sanctions, including an inference that the evidence would have been unfavorable to the destroying party, monetary sanctions against the party and/or its attorney and, in extreme cases, dismissal or default judgment.²¹ Moreover, a party can face similar sanctions by merely failing to preserve relevant evidence, rather than intentionally destroying it.²²

In August 1999, the American Bar Association’s Section of Litigation promulgated Civil Discovery Standards. These standards expressly extend a party’s duty to “preserve potentially relevant documents” to “information contained or stored in an electronic medium or format, including a computer word-processing document, storage medium, spreadsheet, database and electronic mail.”²³ Once a potential dispute arises, therefore, firms should take steps to preserve potentially relevant electronic documents. Depending on the situation, these steps might include some or all of the following:

Identify computer records relevant to the subject matter of the action. These records could include (1) word processing documents (including drafts or versions not in paper form), (2) databases or spreadsheets with relevant information, (3) e-mail, and (4) relevant history records (including logs, internet use history files, and access records).

Locate pertinent computer records. These records could be located in any number of places, including (1) active computer files on network servers, (2) computer files on desktop or local hard drives, (3) backup tapes or disks, (4) archival tapes or disks, (5) laptop computers, home computers, and other “satellite” locations, (6) media or hardware on which relevant records may have been “deleted” but are recoverable using reasonable efforts.

Make sure that all relevant computer records at all locations are secure: (1) suspend all routine electronic document deletion and media recycling, (2) segregate and secure backup and archival media, (3) create “mirror” copies of all active network servers, desktop hard drives, laptops, and similar hardware.

Consider an order to preserve evidence. Although somewhat redundant, parties to litigation often find it beneficial to stipulate to entry of an order for preservation of evidence, to reinforce the obligation to retain relevant documents and other evidence. The consequences of a case-specific preservation order are two-fold: (1) it is far more difficult for a stipulating party to argue that it “inadvertently” deleted or otherwise disposed of relevant evidence; and (2) the penalties for failing to preserve evidence are likely to be more severe, as is usually the case when a litigant violates a court order.

Designate technical “point-persons” who know about the client’s computer systems to assist in managing computer records and answering discovery requests. The firm’s lawyer should interface with the firm’s CIO or IS manager at the outset of the case, rather than after a discovery request has been propounded. Oftentimes the usual “client contact” does not have the technical expertise to ensure that electronic evidence preservation safeguards are properly implemented.

Explore with the client the procedures and costs associated with: (1) locating and isolating relevant files from e-mail, word processing, and other collections, (2) recovering relevant files generated on outdated or dormant computer systems (a.k.a. “legacy data”), (3) recovering deleted relevant files from hard drives, backup media, and other sources.

17.3.3.2 Form of Retention

All electronic document preservation is not alike. In the recent decision of *Zebulke v UBS Warburg*, a federal district court noted that there are five different categories of electronic data (listed from most accessible to least accessible):

1. Active, online data: Data generally provided by magnetic disk, e.g., hard drives. Active, online data exists in the early stages of an electronic record’s life. Relative to other forms of electronic data, access to active, online data is frequent and retrieval is fast.

2. Near-line data: Data stored with robotic devices, and accessed with multiple read/write devices, e.g., magnetic tape. Access is less frequent and slower than active, online data.

3. Offline storage/archives: Data stored in removable optical disk or magnetic tape media that are labeled and physically stored on a shelf or rack. Access is slower because it requires manual intervention.

4. Backup tapes: Tape drives with large capacity, but that are generally unable to access data selectively because the data is stored sequentially, i.e., to read any specific data, one must review all preceding data. Backup tapes commonly employ data compression, which enlarges storage capacity but makes retrieval more time-consuming and expensive.

5. Erased, fragmented or damaged data: Clusters of files made available as “free space” after deletion, or broken up and dispersed throughout a data disk. These files can only be accessed after very lengthy and expensive processing.²⁴

The form of electronic data retention – including when data progresses from one form to another – is an essential ingredient of a document retention program. Generally speaking, the less data is active, accessible and integrated, the more expensive its retrieval. This becomes very important when, in the context of a lawsuit, one party seeks electronic data that has been archived and can only be retrieved at great expense. More and more frequently, courts are being asked to decide who must pay for the cost of retrieval.

There is a general presumption that the producing party must pay for the costs of producing records, though this presumption may be overcome by a responding party's request under the discovery rules to protect the responding party from undue burden and expense. *Oppenheimer Fund, Inc v Sanders*, 437 US 340, 358, 57 L Ed 2d 253, 98 S Ct 2380 (1978). More recently, courts have applied a number of factors to determine whether the presumption should be overcome so as to require the requesting party to pay some or all the costs of retrieval of electronic evidence. The stakes can be quite high. Indeed, retrieval costs in some instances can reach hundreds of thousands, and even millions, of dollars. The leading case on the retrieval cost issue is *Rowe Entertainment, Inc v The William Morris Agency*, 205 FRD 421 (SDNY 2002). In *Rowe*, the court fashioned an eight-part test that subsequent courts have followed in its entirety or with slight modifications. The *Rowe* test balances:

- (1) the specificity of the discovery requests;
- (2) the likelihood of discovering critical information;
- (3) the availability of such information from other sources;
- (4) the purposes for which the responding party maintains the requested data;
- (5) the relative benefit to the parties of obtaining the information;
- (6) the total cost associated with production;
- (7) the relative ability of each party to control costs and its incentive to do so; and
- (8) the resources available to each party.²⁵

Because of variations in facts, it is difficult to predict how a court would rule on such an issue in a specific case. The important point is that when designing an electronic document retention policy, a firm should consider how long it needs to retain such data and, if retained, the cost of restoring it to usable form.

17.3.3.3 Special Document Retention Considerations for Construction Firms

Because of the nature of their business, construction firms often impulsively “move on to the next project” without considering how to preserve electronic records generated from the project just completed. Data on floppy and Zip disks, CD-ROMs, and stand-alone, non-networked computers are especially susceptible to being destroyed or overwritten at the conclusion of a project. Construction firms should craft and enforce a policy to collect and preserve all such data at the conclusion of each project.

17.3.4 Submitting to Jurisdiction through e-Commerce

There have been a number of recent attempts by claimants in other states to hail out-of-state companies into their home states' courts on the basis that the defendant's web site, accessible in that state, constitutes a “presence” sufficient to confer personal jurisdiction in that forum. In most instances, companies are held not to have agreed to be sued in other states merely by having a web site on the World Wide Web. Nevertheless, courts have held that where the web site is interactive, i.e., where the site allows users to download, transmit or exchange information with the company via computer, or where the user has entered into an on-line contract with the company, such contacts can be sufficient to confer personal jurisdiction. See, e.g., *Audi AG & Volkswagen of America, Inc v Izumi*, 204 F Supp 2d 1014, 1020-1021 (ED Mich 2002). For internet retailers, such interaction is a necessary component of everyday business. For construction firms, the necessary degree of interactivity will vary. When designing a web site, firms should weigh the benefits of interactivity against the risks that the firm could be hailed before a distant state's court.

17.3.5 Cyber Court

In 2001, to great fanfare, the Michigan Legislature created the Michigan Cyber Court.²⁶ The Cyber Court is designed as an optional forum for business litigants who wish to avail themselves of a true virtual courtroom. For instance, in the Cyber Court, parties appear by videoconference, pleadings and papers are filed online, and status conference are conducted by e-mail. Proceedings are “public” in the sense that they may be heard on the Internet.²⁷ Unfortunately, the Cyber Court fell prey to budget cuts.²⁸ As and

when it is funded, it will be interesting to see how the high-tech environment is accepted by business, and whether it fulfills its promise as a more efficient vehicle for dispute resolution.

17.3.6 Technology in the Workplace

While technology has offered excellent tools to improve worker productivity, it ironically also provides opportunities for worker distraction and temptation. Employers inside and outside of the construction industry are trying to rein in excessive personal use of the Internet (including e-mail and on-line shopping and browsing), cell phones, and computer games. Prudent companies appreciate this dilemma and publish explicit restrictions on unreasonable personal (and possibly illegal) use of employer-provided technology. While each company should consult an attorney to develop a policy suitable to its needs, such a policy might include the following points:

Computers, telephones, voice mail, e-mail and other employer-provided technology are the property of the employer.

The employer has the right to review, delete or otherwise make use of any information stored on e-mail, voice mail and other employer-provided technology systems.

Personal use of employer-provided technology is limited in some quantified manner, e.g., less than 5% of total use (or prohibited). Where personal use of technology is permitted, the employer may at any time review, delete or otherwise make use of the information, and employees should not have any expectation of privacy relative to personal, as well as business, use of employer-provided technology.

No employer-provided technology may be used for any improper purpose, including but not limited to unlawful activities, defamation or harassment of others, display of sexually-explicit, obscene or offensive images, racially insensitive or other insulting messages, and the like.

Violation of the policy on employer-provided technology can lead to disciplinary action, up to and including discharge.

17.3.7 Computer Security

Computer security has potentially far-reaching legal, as well as business, implications. Good security is good business, whether in terms of preventing inventory “shrinkage,” improving employee safety, or thwarting industrial espionage, malicious hackers, and computer viruses. Construction firms, like other businesses, need to implement appropriate security safeguards in order to alleviate risk of loss (direct and indirect) due to security breaches.

Every computer system carries a degree of security risk. Computer security risk increases with interconnectivity of the computer systems of various players in a construction project. Thus, the principal operational advantage of an integrated project management system can also prove to be its greatest weakness. Corruption or shutdown of an integrated project management site could have disastrous schedule and cost consequences to the parties and the project alike.

Specific computer security technology is beyond the scope of this chapter. Nevertheless, as a critical business management issue, the risks and benefits of computer security should be well understood. In this regard, firms are commended to the U.S. Department of Commerce’s Special Publication 800-12, entitled “An Introduction to Computer Security: The NIST Handbook,” published by the National Institute of Standards and Technology.

The NIST Handbook takes a pragmatic approach to computer security that is based on eight major elements:

1. Computer security should support the mission of the organization.
2. Computer security is an integral element of sound management.
3. Computer security should be cost-effective.
4. Computer security responsibilities and accountability should be made explicit.
5. System owners have computer security responsibilities outside their own organizations (i.e., system owners should apprise clients and outside users about the general nature and extent of security measures and act promptly to protect clients from security breaches).
6. Computer security requires a comprehensive and integrated approach.
7. Computer security should be periodically reassessed.
8. Computer security is constrained by societal factors (i.e., security needs to be balanced with workplace privacy concerns).²⁹

17.4 Conclusion

Business processes, laws, and the judicial system continue to adapt to information technology's "sharp transformation" of western civilization. While information technology has made business faster, cheaper, and more efficient, it has also made business management and the practice of law more challenging and complex.

¹ Porter, Millar, *How Information Gives You Competitive Advantage*, Harvard Business Review (July-August 1985).

² Kanellos, *Moore's Law to Roll On for Another 10 Years*, C/Net News.Com (February 10, 2003), available at <http://news.com.com/2100-1001-984051.html>.

³ *Id.*

⁴ Raczkowski, *Voice Portals: Adding a Human Touch to the Web* (dash30 2002), available at <http://global.mci.com/resources/whitepapers/pdf/VoicePortals.pdf>.

⁵ PhD candidate Pollaphat (Frank) Nitithamyong is conducting the research. Article and survey available at http://www.constructionweblinks.com/Resources/Industry_Reports__Newsletters/June_30_2003/purdue.htm.

⁶ *Michigan Department Of Transportation Leads Nation In Implementing Internet Bidding*, http://www.michigan.gov/mdot/0,1607,7-151-9620_11057-25830--M_2002_2,00.html.

⁷ *Id.*

⁸ The act expressly does not apply to a transaction to the extent governed by (a) laws relating to the creation and execution of wills, codicils, or testamentary trusts, or (b) by the Uniform Commercial Code, except to the extent the transaction is governed by Articles 2 (sale of goods) or 2A (leases), or Sections 1107 (MCL 440.1107) or 1206 (MCL 440.1206). MCL 450.833(2), (3).

⁹ MCL 450.835; 450.837.

¹⁰ MCL 450.842; 450.843.

¹¹ <http://enr.construction.com/news/informationtech/archives/030616.asp>

¹² See, Davenport, *Putting the Enterprise into the Enterprise System*, Harvard Business Review (July-August 1998), Reprint No. 98401.

¹³ See, e.g., *Zubulake v UBS Warburg*, 2003 US Dist LEXIS 7939 at *4 (SDNY 2003) (in employment discrimination and retaliation case, supervisor e-mail suggested that the plaintiff be fired "ASAP" after her EEOC charge was filed, in part so that she would not be eligible for year-end bonuses).

¹⁴ Document retention is yet more complicated because of uncertainty as to whether electronic data has been "deleted" but still recoverable. One court recently explained:

The term "deleted" is sticky in the context of electronic data. "Deleting" a file does not actually erase that data from the computer's storage devices. Rather, it simply finds the data's entry in the disk directory and changes it to a 'not used' status -- thus permitting the computer to write over the 'deleted' data. Until the computer writes over the 'deleted' data, however, it may be recovered by searching the disk itself rather than the disk's directory.

Accordingly, many files are recoverable long after they have been deleted -- even if neither the computer user nor the computer itself is aware of their existence. Such data is referred to as 'residual data.'" Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. Rev. 327, 337 (2000) (footnotes omitted). Deleted data may also exist because it was backed up before it was deleted. Thus, it may reside on backup tapes or similar media. *Zubulake v UBS Warburg*, 2003 US Dist LEXIS 7939 (fn 19) at *10 (SDNY 2003).

¹⁵ *Antioch Co v Scrapbook Borders, Inc*, 210 FRD 645, 652 (D Minn 2002).

¹⁶ 48 CFR 4.703. Similarly, 36 CFR 64.11 and 38 CFR 43.36 require records retention for certain Department of Interior and Veterans Affairs projects for three years after final payment.

¹⁷ MCL 600.5807(8).

¹⁸ MCL 600.5839. Note that if the contractor is guilty of gross negligence, however, the statute is extended to one year after the defect is discovered or should have been discovered, with the exception that no such action may be maintained more than 10 years after the time of occupancy of the completed improvement, use, or acceptance of the improvement.

¹⁹ *See, e.g., Brenner v Kolk*, 226 Mich App 149, 162, 573 NW2d 65 (1997) ("Even when an action has not been commenced and there is only a potential for litigation, the litigant is under a duty to preserve evidence that it knows or reasonably should know is relevant to the action").

²⁰ *See, e.g., Proctor & Gamble v Haugen*, 179 FRD 622 (D Utah 1998) (sanctioning plaintiff for failing to preserve the e-mails of five individuals who were identified by the opposing party as possibly having information relevant to the litigation, even through at the time of destruction there was no pending discovery request and the court did not find that the e-mails were destroyed in bad faith).

²¹ *Trupiano v Cully*, 349 Mich 568, 84 NW2d 747 (1957).

²² *E.g., Boemendaal v Town & Country Sports Center Inc*, 255 Mich App 207, 659 NW2d 684 (2002) (dismissal of product liability action for failing to preserve evidence).

²³ Civil Discovery Standard 29 a. i. (American Bar Association, 1999).

²⁴ *Zubulake*, 2003 U.S. Dist. LEXIS 7939 at *30-33, citing Cohasset Associates, Inc. White Paper: Trustworthy Storage and Management of Electronic Records: The Role of Optical Storage Technology (April 2003); CNT, the Future of Tape 2, available at <http://www.cnt.com/literature/documents/pl556.pdf>; Webopedia, at http://inews.webopedia.com/TERM/t/tape_drive.html; Kenneth J. Withers, Computer-Based Discovery in Federal Civil Litigation; SDLT, Inc., Making a Business Case for Tape, at http://quantum.treehousei.com/Surveys/publishing/survey_14making_a_business_case_for_tape.pdf; Jerry Stern, The Perils of Backing Up, at http://www.grsoftware.net/backup/articles/jerry_perils.html; Sunbelt Software, Inc., White Paper: Disk Defragmentation for Windows NT/2000: Hidden Gold for the Enterprise 2, at <http://www.sunbeltsoftware.com/evaluation/455/web/documents/idcwhitepaper-english.pdf>; Executive Software, Inc., Identifying Common Reliability/Stability Problems Caused by File Fragmentation, at http://www.execsoft.com/Reliability_Stability_Whitepaper.pdf; Stan Miastkowski, When Good Data Goes Bad, PC World, Jan. 2000, available at <http://www.pcworld.com/resource/printable/article/0,aid,1385asp>.

²⁵ *Rowe*, 205 FRD at 429.

²⁶ *See*, MCL 600.8001, *et seq.*

²⁷ *See*, Ponte, *The Michigan Cyber Court: A Bold Experiment in the Development of the First Public Virtual Courthouse*, 4 N.C. J.L. & Tech. 51 (2002).

²⁸ *See*, Lane, *Lack of Funding Keeps Cyber-Court Offline*, Michigan Craintech (July 15, 2002), article available at <http://michigancraintech.com/cgi-bin/articl.pl?articleId=2163>.

²⁹ For more information, visit the NIST's Computer Security Resource Center at <http://csrc.nist.gov/>.