WHEN DOCUMENT RETENTION REQUIREMENTS COLLIDE WITH ELECTRONICALLY STORED INFORMATION

By E. Ray Stanford, Jr.
Irvin, Stanford & Kessler, LLP
3060 Peachtree Road
Suite 1050
Atlanta, Georgia 30305
rstanford@isklaw.com

WHEN DOCUMENT RETENTION REQUIREMENTS COLLIDE WITH ELECTRONICALLY STORED INFORMATION! *

TABLE of CONTENTS †

I. INTRODUCTION ... 4
  A. Paper Document ... 7
  B. Electronically Stored Information ... 9
  C. Possessed Workplace Information (PWI) ... 10
III. PWI CATEGORIES ... 11
  A. Traditional Documents ... 11
  B. ESI Sources ... 12
IV. WORKPLACE DOCUMENT RETENTION LAWS ... 14
  A. Traditional Document Retention Laws ... 14
    1. Fair Labor Standards Act and Equal Pay Act of 1963 ... 14
    2. Family and Medical Leave Act (“FMLA”) ... 15
    3. Title VII of the Civil Righ ts Act of 1964 (“Title VII”) ... 16
    4. Age Discrimination in Employment Act of 1967 (ADEA) ... 18
    5. Civil Rights Act of 1866 ... 19
    6. Americans with Disabilities Act (“ADA”) ... 19
    7. Employee Retirement and Insurance Security Act (“ERISA”) ... 19
    8. Occupational Safety and Health Act (OSHA) ... 21
    9. OFCCP-Executive Orders ... 21
    10. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) ... 22
    11. Sarbanes-Oxley Act of 2002 ... 22
    12. The Immigration Reform and Control Act of 1986 (IRCA) ... 23
    13. Employee Polygraph Protection Act ... 24
    14. Federal Withholding, Unemployment, and Social Security Requirements ... 24
    15. Fair and Accurate Credit Transactions Act (FACTA) ... 25
    16. Spoliation [RS add] ... 25
    17. 2005 Proposed E-Amendments to the FRCP ... 26
V. RECOMMENDATIONS ... 32
  A. PWI Retention Systems ... 32

* ©July 1, 2005, Ray Stanford, Irvin, Stanford & Kessler, LLP

† The author gratefully acknowledges and appreciates the invaluable assistance of Thomas Wooldridge, 2L Southern Illinois Law School, Teresa Hearn, and Catherine Stanford.

1. Identify All Categories of PWI 33
2. Identify All Legally Mandated PWI Retention Periods 33
3. Establish Additional Retention Periods 33
4. Routinely Destroy PWI 34
5. Include All Sources of PWI 34
6. Suspend Routine Destruction for Potential Litigation 34

B. Investigations 35

C. Litigation Responses 37

VI. CONCLUSION 38

VII. APPENDIX: CHART OF RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS 39

I. INTRODUCTION

This article focuses on the intended and unintended consequences that electronically stored information (ESI)[‡] and its related entourage of E-laws have on human resource, have on document retention programs. The term "possessed workplace information" (PWI) has been adopted to cover all workplace information that might be the target of legal retention requirements and strategies pertaining to information of a particular employer. Traditional laws imposing information retention requirements on employers typically deal with "documents" or "records". Newer laws have tended to focus on ESI and E-docs without offering a catch-all phrase or term. For the time being, and in this article, PWI will serve this catch-all role.

While information gathering and preservation remains a major phase of any successful operation, the proliferation of data threatens to suffocate the workplace[§]. The explosion of captured data creates a number of problems for business ranging from the feasibility of housing and handling the data to paying for it. Although properly leveraging information can pay dividends for companies, the malignant spread of data brings uncertainty, added costs, poorer productivity, higher turnover, and increased tension to the workplace. To deal with the growth of data, companies have begun to develop (or purchase) "document retention programs".[**] While these document retention programs help organize ESI, the programs often compete with a company's profit mission.

[‡] The Report of Civil Rules Advisory Committee of the Standing Committee on Rules of Practice and Procedure (May 27, 2005) ("2005 FRCP Report") uses the phrase "electronically stored information" (ESI) and distinguishes it from information stored on paper documents. This article adopts the same phraseology.

[§] A typical floppy disk, a standard storage unit a few years ago, could hold around 720 typewritten pages; while a 650 megabyte CD-ROM can hold around 325,000 typewritten pages. Large information backup systems can hold data measured in terabytes (1 million megabytes). A system storing a terabyte of data stores the equivalent of 500 million typewritten pages. Manual for Complex Litigation (4th) § 11.446 cited in 2005 Civil Rules Report.

[**] For an in-depth discussion of document retention programs see Corporate Compliance Series: Designing An Effective Records Retention Compliance Program, J. Edwin Dietal,

Apart from the practical problems that accompany the growth in data, the legal duties governing information handling systems add another layer of concern for business. In relatively recent times,[††] laws and regulations have imposed a complex patchwork of document retention requirements on employers. For example, covered employers must preserve gender information for 2 years,[‡‡] age information for 3 years,[§§] and race information permanently.[***]

As the law attempts to keep up with the development of electronic information, business has suffered new and sometimes bizarre legal regulation of electronically stored information. In recent years, the workplace has welcomed the legal supervision of ESI from a variety of laws such as Sarbanes-Oxley,[†††] Fair and Accurate Credit Transactions Act ("FACTA") [‡‡‡], and the USA Patriot Act. The maturing concept of spoliation and the proposed amendments to the federal rules of civil procedure contained in the 2005 FRCP Report add to business's challenge of handling both paper documents and ESI.

Section II of the article explores the traditional definitions of a document and whether the definitions contemplate ESI. As expected, many of the older laws do not address ESI. Although courts have begun to provide some guidance regarding the meaning of a document and ESI, many traditional retention laws have not been amended or interpreted to explain the meaning of a document in the information age. Section II then reviews more recent definitions of workplace information such as electronic

[††] Colonial business bore some legal duty to preserve business records. For example, the Stamp Act of 1765 imposed levies on colonial newspapers and newspaper advertisements and a related obligation to identify the papers and advertisements subject to the Act. 5 Geo. III, ch. 12, § 1. (Parliament had previously imposed a similar tax on British newspapers in 1712. 10 Anne, ch. 18, § 113.) Still, for most early American businesses, the retention of business information flowed from a practical need rather than a legal mandate.

[‡‡] 29 C.F.R. § 1602.12 and 29 C.F.R. 1620.32.

[§§] 29 C.F.R. § 1627.3.

[***] 29 C.F.R. § 1602.13.

[†††] 18 U.S.C.A. § 1514A et seq.

[‡‡‡] 15 U.S.C.A. §1681 et seq.

documents and ESI. These new efforts to categorize workplace information either deal exclusively with ESI or simply recognize ESI as a subset of the larger category of workplace information. The term possessed workplace information (PWI) has been adopted to cover all information possessed by a business.

Unlike most legal analysis of PWI systems, this article also addresses the retention requirements and the impact of technology from the perspective of the categories of information rather than a particular law. Instead of focusing exclusively on the retention specifics mandated by statutes such as Title VII, Sarbanes-Oxley, and FLSA, portions of this article analyze technology and retention requirements by considering the impact of ESI laws on the retention requirements of a particular human resource category of PWI such as employment applications, credit information, affirmative action plans, and other PWI categories.[§§§] To provide a framework for human resource-related PWI, section III groups PWI into categories that should be familiar to most employment lawyers and human resource professionals.

Section IV offers an updated list of laws that bear on the retention requirements for each human resource category of PWI. For example, retention laws that relate to hiring PWI include Title VII, FLSA, HIPAA, ADEA, FLSA, FCRA, ADA, and various AAP executive orders.[****] Section IV continues the exploration of legal PWI retention requirements by asking

[§§§] Asking how should hiring PWI be handled rather than what are the retention requirements of Title VII tends to redirect the inquiry to the practical concerns of business rather than the narrow interests of the law. To continue the introductory example involving race, sex, and age, how should an employer store identifying information of a Hispanic, 55 year-old, female employee? If the employee subsequently asserts a claim for race, sex, and age discrimination will the employer be required to produce all sources of PWI relating to the race, sex, and age of the worforce or simply the employee's personnel file.

[****] Plaintiff counsel, as well as defense counsel, has a stake in understanding workplace information retention requirements. For example, Plaintiff attorneys who understand the nuances of information retention programs will be able to engage in effective and focused discovery and exert increased litigation pressure.

whether and, if so, how the traditional laws and regulations deal with ESI. More recent laws, regulations, and other concepts relating to PWI such as Sarbanes-Oxley, the proposed amendments to the federal rules of procedure, and spoliation have been added to the list. To help connect the human resource categories of PWI with the legal retention requirements, the Appendix contains a chart listing the human resource categories of PWI and the related retention laws and regulations.

A final section offers recommendations for dealing with the emerging interplay between ESI and ESI-related laws, and PWI retention needs for human resources.

II. LEGAL DEFINITIONS OF DOCUMENTS, ESI, AND POSSESSED WORKPLACE INFORMATION (PWI)

A. Paper Document.

An obvious challenge exists when traditional laws dealing with "documents" are applied to workplaces in the new information age. If a law defines a document as a tangible item (e.g., paper) on which information has been recorded, the law omits other mediums of retained information (like a website). Some laws refer to documents (some to records) without offering any meaning to the term document. The following list illustrates the range of definitions of the word document:

- An instrument on which is recorded, by means of letters, figures or marks, the original, official, or legal form of something, which may be evidentially used. In this sense the term document applies to writings; to words printed, lithographed, or photographed; to maps or plans; to seals or plates or even stones on which inscriptions are cut or engraved.[††††]
- Something tangible on which words, symbols, or marks are recorded.[‡‡‡‡]

[††††] Black's Law, 5th Ed. 1979.
[‡‡‡‡] Blacks Law 8th Ed. 2004 citing to Fed. R. Civ. P. 34(a)

- Any physical embodiment of information or ideas -- a letter, a contract, a receipt, a book of account, a blueprint, or an X-ray plate.[§§§§]

In some legal schemes, the term "document" and "record" are used interchangeably. In other contexts, "record" appears as a subset of a "document" as when a document is defined as "any physical embodiment of information or ideas" and necessarily includes records.[*****] The Federal Rules of Evidence make numerous references to records and documents as both distinct but overlapping concepts. The hearsay exceptions contained in Rule 803 include various types of "records":

(6) Records of regularly conducted activity. A memorandum, report, record, or data compilation … of acts … kept in the course of a regularly conducted business activity …;
(8) Public records and reports. Records, reports, statements, or data compilations … of public offices or agencies …;
(9) Records of vital statistics. Records or data compilations … of births, fetal deaths, deaths, or marriages …;
(11) Records of religious organizations. Statements of births, marriages, divorces, deaths … contained in a regularly kept record of a religious organization.[†††††]

Rule 1005 defines a "Public Record" as

> The contents of an official record or of a document authorized to be recorded or filed and actually recorded or filed, including data compilations in any form.[‡‡‡‡‡]

[§§§§] Strico v. Cotto, 324 N.Y.S.2d 483, 486 (Civ. Ct. 1971) (defining document within the meaning of the Best Evidence Rule).
[*****] Hon. Shira A. Scheindlin & Jeffrey Rabkin, Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?, 41 B.C. L. Rev. 327, 333 (2000) ("Scheindlin, Electronic Discovery") (citing Strico v. Cotto, 324 N.Y.S.2d 483, 486 (Civ. Ct. 1971)).
[†††††] Fed. R. Evid. 803.
[‡‡‡‡‡] Fed. R. Evid. 1005.

In other contexts, documents and records seem to be given different meanings. Some document retention programs separate the concept of “document management” from “records management.” In document management systems, the creator (and other users) may access and change the document. In a records management system, once the user declares a document to be a record, the central organization, not the creator, assumes responsibility for managing the records.[§§§§§]

B. Electronically Stored Information.

Responding to the influx of document-focused lawsuits, courts and legislatures have begun to wrestle with the universe of information found in the workplace. To begin the process of ordering the new category of electronically stored information[******], various labels have been assigned to this subset of workplace information. For example, “electronic document” and “electronic data” have been used to encompass all types of electronic information possessed by a party.[††††††] In adopting the term electronic document in the context of Rule 34, one author explained,

---

[§§§§§] Document Management (DM) and Records Management (RM). Corporate Compliance Series: Designing An Effective Records Retention Compliance Program, Edwin Dietal, § 3:89 (2004); see The New Shorter Oxford English Dictionary 2056 (1993). (A record is an account of information or facts set down in writing to preserve knowledge.) Most review articles tend to interchange the words “record” and “document.”

[******] For example, electronic data has been categorized as: active date, metadata, replicate data, residual data, backup data, and legacy data. Marilee S. Chan, Paper Piles to Computer Files: A Federal Approach to Electronic Records Retention and Management, 44 Santa Clara L. Rev. 805, 812 (2004).

[††††††] See Zubulake v. UBS Warburg, 220 F.R.D. 212 (S.D.N.Y. 2004) and FG Hemisphere Associates, LLC v. Republique Du Congo, 2005 WL 545218 (S.D.N.Y. 2005). Other agencies use the same or similar terms to cover electronic information. In the context of the use of electronic information in the administration of agricultural warehouses, Congress has defined an “electronic document” as “any document that is generated, sent, received, or stored by electronic, optical, or similar means, including, but not limited to, electronic data interchange, advanced communication methods, electronic mail, telegram, telex, or telecopy.” 7 USCS § 241.

> [We use the term "electronic document" to refer to a subset of electronic evidence: information intentionally created by a computer user … and stored in electronic form. The term electronic document comes about naturally because the word "document" has been defined broadly in other legal contexts as "any physical embodiment of information or ideas." (Citation omitted.) By using the modifier "electronic," the term incorporates the idea that the "physical embodiment of information or ideas" must be kept in electronic form—or … in the form of binary numbers stored on electric transistors.[‡‡‡‡‡‡]

Acknowledging the plethora of labels and information categories, the 2005 FRCP Report adopts "electronically stored information" (ESI) as a discoverable category of information separate from a document.[§§§§§§]

C. Possessed Workplace Information (PWI).

The phrase "possessed workplace information" (PWI) has been adopted to cover all types of workplace information possessed by an employer. The word "document" has been used too often to mean paper and invites confusion if a document is deemed to cover all types of data compilations. The phrase ESI, e-docs, and other electronic related terms omit paper and other tangible forms of data compilations. Use of the word "possessed" carries some legal understanding that attributes to the possessor some connection with the "possessed" information.[*******] Thus, PWI has

---

[‡‡‡‡‡‡] Scheindlin, Electronic Discovery, 333.

[§§§§§§] See section IV.A.18. , infra. If a request for production seeks only" documents", proposed Rule 34(a) would require "the responding party [to] produce responsive information no matter what the storage form may be." 2005 FRCP Report § I.C.2.iv.. The Committee Note to proposed Rule 34 provides:

> [A] request for production of "documents" should be understood to encompass, and the response should include, electronically stored information unless discovery in the action has clearly distinguished between electronically stored information and documents.

[*******] The scientific qualities of ESI raise questions about the scope of an employer's "possession, custody, or control" of ESI. Rule 34's production requirements of a party

been selected as a workable term for all information within the possession of a particular employer.

III. PWI CATEGORIES

A. Traditional Documents.

To provide a perspective that more closely mirrors the real-world views of an employer or human resource professional, a first step in the development of a PWI retention system should be a catalogue of categories of human resource PWI. The following categories of PWI have been offered as a workable summary of human resource categories of PWI:

1. Race, Ethnic Identity: (optional) post-employment record, if permitted by state law.
2. Gender Identity: gender based pay records
3. Age Identity
4. Veteran Identity
5. Application, resumes, response to job ads
6. Hiring Documents (also rejection documents)
7. Position/Job Description
8. Compensation: Payroll (name, address, DOB, occupation, weekly compensation); individual contracts, collective bargaining agreements, notices of Wage-Hour/Supplemental records- wage rate tables; work time schedules; order, shipping, billing records; wage addition or deduction records. Certificates of Age.
9. Benefits: general/benefit plans, seniority merit systems.
10. I-9, Eligibility and Verification documents
11. Investigation: Criminal

---

within the "possession, custody, or control" of the requested document or ESI carries the legal assumption that the employer not only has some connection with the document/ESI, but should bear some legal responsibility for the production of the document/ESI. Do the attributes of ESI alter the appropriateness of this assumption? For example, if an employer's handbook declares that all employees consent to searches of any and all items taken into the workplace, should the employer be deemed to have possessed or controlled the information that came across an employee's PDA during worktime?

12. Investigation: Financial
13. Investigation: Education
14. Investigation: Employment History
15. Safety and Health
16. Medical: Medical condition or history, Examinations
17. Selection PWI- Employers <100 employees
18. Selection PWI - Employers $100 employees
19. Selection for training or apprenticeship (not apprenticeship records)
20. Leave records of FMLA compliance, e.g. dates and hours of leave taken, notices, leave policies and benefits, leave disputes
21. Requests for reasonable accommodation
22. Performance
23. Promotion/Transfer
24. Discipline/Demotion
25. Lay-off
26. Termination
27. Ethics
28. Executives (CEO)
29. Board of Directors
30. Temporary Workers(same as for regular employees plus job orders submitted to agencies or unions)
31. Claims, charges, lawsuits
32. Contract Worker PWI
33. Required Reports: EEO-1
34. Required Reports: Affirmative action plans and supporting PWI
35. Personnel and employment records of federal contractors with 150 or more employees and $150,000 contract

B. <u>ESI Sources</u>.

The development of electronic information has created new locations or “sources” for ESI. Although these sources may not create new categories of PWI subject to separate retention requirements, the ESI and related

storage media do affect the legal retention and production requirements of PWI. See section IV.A.17 below, for a discussion of the proposed FRCP amendments dealing with ESI and discovery. New electronic sources include:

1. E-Mail
2. Electric fingerprints
3. Electric voice recognition
4. Electric signatures
5. Metadata
6. Cookies
7. Ghosts
8. Instant messages
9. Attachments to documents
10. Backup tapes
11. Backup servers
12. Obsolete software
13. Handheld devices
14. Employee laptops
15. Optical discs
16. Voicemail
17. Backup directories
18. Desktop computers at employee workstations
19. Personal digital assistants
20. Home computers
21. Floppy disks
22. Hard drives
23. Digital camera's
24. Web sites
25. Extranets
26. Cache files
27. Internet browser history files
28. Site log files
29. Bookmarks
30. Favorite places
31. Remote locations containing the same sources as above.

IV. WORKPLACE DOCUMENT RETENTION LAWS

A. Traditional Document Retention Laws

The following summary of document retention laws illustrates various and imprecise use of the words "document" and "record". With the exception of a few statutory schemes, the traditional retention laws do not address ESI.[†††††††]

1. Fair Labor Standards Act and Equal Pay Act of 1963

The Fair Labor Standards Act ("FLSA") divides "record" retention into 2 and 3 year categories. An employer must maintain for 3 years:

- all payroll and other information containing the employee's name, address, birth date,
- compensation agreements including collective bargaining agreements;
- the company's total "sales and purchases."[‡‡‡‡‡‡‡]

"Basic employment and earnings records" must be kept for 2 years.[§§§§§§§] This catch-all category includes wage rate tables and schedules, basic time and earnings cards or sheets containing starting and ending times or amounts of work accomplished on a daily, weekly or month basis and records of changes to wages.[********] The FLSA also requires an employer to preserve for 3 years all "order, shipping, and billing records."[††††††††]

As the enforcement agency for record keeping requirements under the Equal Pay Act, the EEOC simply requires compliance with the

---

[†††††††] An interesting conflict could arise between the imprecise retention requirements of a traditional document retention law and the better defined requirements of spoliation laws and the proposed amendments to the FRCP.

[‡‡‡‡‡‡‡] 29 C.F.R. § 516.5.

[§§§§§§§] 29 C.F.R. § 561.6.

[********] Id.

[††††††††] Id.

FLSA record-keeping standards.[‡‡‡‡‡‡‡‡] "In addition" to the FLSA requirements, an employer must preserve for two years

> any records … which relate to the payment of wages, wage rates, job evaluations, job descriptions, merit systems, seniority systems, collective bargaining agreements, description of practices or other matters which describe or explain the basis for payment of any wage differential to employees of the opposite sex in the same establishment, and which may be pertinent to a determination whether such differential is based on a factor other than sex.[§§§§§§§§]

The FLSA regulations do not prescribe a particular order or form of record retention but employers may preserve records on microfilm or in word processing programs, as long as the reproductions are clear and identifiable by date or pay period and that extensions or transcriptions of the information required by this part are made available upon request.[*********]

2. Family and Medical Leave Act ("FMLA")

Regulations issued pursuant to the FMLA require covered employers to "make, keep, and preserve records pertaining to their obligations under the FMLA.[†††††††††] The regulations incorporate the FLSA recordkeeping scheme and require employers to maintain the following "records" for three years:

> (1) Basic payroll and identifying employee data, including name, address, and occupation; rate or basis of pay and terms of compensation; daily and weekly hours worked per pay period; additions to or deductions from wages; and total compensation paid.

[‡‡‡‡‡‡‡‡] 29 C.F.R. § 1620.32.
[§§§§§§§§] Id.
[*********] 29 C.F.R. § 516.1(a)
[†††††††††] 29 C.F.R. § 1620.32.

> (2) Dates FMLA leave … taken by. eligible employees (e.g., available from time records, requests for leave, etc. ….
> (3) [Incremental leave records.]
> (4) Copies of employee [leave notices] and specific written notices given to employees as required under FMLA …Copies may be maintained in employee personnel files.
> (5) Any documents (including written and electronic records) describing employee benefits or employer policies and practices regarding the taking of paid and unpaid leaves.
> (6) Premium payments of employee benefits.
> (7) Records of [leave disputes between the employer and an eligible employee.][‡‡‡‡‡‡‡‡‡]

FMLA medical "records and documents" of employees or employees' family members must be kept confidential in "file/records" separate from the usual personnel files.[§§§§§§§§§] FMLA regulations do not specify a record-keeping form, but do allow records to be maintained and preserved on "microfilm or other basic source document of an automated data processing memory."[**********]

3. Title VII of the Civil Rights Act of 1964 ("Title VII")

Although EEOC regulations declare that the Commission has not adopted any requirement that "records be made or kept"[††††††††††], the EEOC does require covered employers to maintain a copy of its most recently filed EEO-1 report.[‡‡‡‡‡‡‡‡‡‡] If an employer does obtain information regarding an employee's race or ethnicity, the "record"should be kept permanently and

> separately from the employee's basic personnel form or other records available to those responsible for personnel

[‡‡‡‡‡‡‡‡‡] Id.
[§§§§§§§§§] 29 C.F.R. § 825.500(g).
[**********] 29 C.F.R. § 825.500(b)
[††††††††††] 29 C.F.R. §1602.12.
[‡‡‡‡‡‡‡‡‡‡] 29 C.F.R. §1602.07.

> decisions, e.g., as part of an automatic data processing system in the payroll department.[§§§§§§§§§§]

Regulations also require preservation for 1 year:

- from the date of creation or personnel decision, [any] "personnel or employment record made or kept by an employer (including but not necessarily limited to requests for reasonable accommodation, application forms submitted by applicants and other records having to do with hiring, promotion, demotion, transfer, lay-off or termination, rates of pay or other terms of compensation, and selection for training or apprenticeship)"; and
- from the date of termination, "personnel records" of any involuntary termination.[***********]

Finally the Title VII regulations require preservation of all "personnel records relevant to the charge or action" until the matter has been resolved. The term "personnel records relevant to the charge or action" include

> personnel or employment records relating to the aggrieved person and to all other employees holding positions similar to that held or sought by the aggrieved person and application forms or test papers completed by an unsuccessful applicant and by all other candidates for the same position as that for which the aggrieved person applied and was rejected.[†††††††††††]

EEOC policy guidance regarding internet related technologies deals with e-mail communications, job postings on the internet, resume databases, job banks, electronic scanning technology, and applicant tracking

---

[§§§§§§§§§§] 29 C.F.R. §1602.13.
[***********] 29 CFR 1602.14.
[†††††††††††] Id.

systems. Although discussing forms of ESI, the EEOC's guidance does not make any meaningful distinction between paper and ESI.

4. Age Discrimination in Employment Act of 1967 (ADEA)

As the enforcing agency of the ADEA, the EEOC has adopted the FLSA's 3-year retention requirements for payroll and other records containing an employee's identity information.[‡‡‡‡‡‡‡‡‡‡‡] In addition, employers must keep for one year the following "employment records":

- Job applications, resumes, or any other form of employment inquiry whenever submitted to the employer in response to his advertisement or other notice of existing or anticipated job openings, including records pertaining to the failure or refusal to hire any individual,
- Promotion, demotion, transfer, selection for training, layoff, recall, or discharge of any employee,
- Job orders submitted by the employer to an employment agency or labor organization for recruitment of personnel for job openings,
- Test papers completed by applicants or candidates for any position which disclose the results of any employer-administered aptitude or other employment test considered by the employer in connection with any personnel action,
- Results of any physical examination where such examination is considered by the employer in connection with any personnel action,
- Any advertisements or notices to the public or to employees relating to job openings, promotions, training programs, or opportunities for overtime work, and
- Any employee benefit plan, seniority and merit system.[§§§§§§§§§§§]

---

‡‡‡‡‡‡‡‡‡‡‡ 29 C.F.R. § 1627.3.

§§§§§§§§§§§ Id.

No particular order or form of records is required by the ADEA or the regulations enforcing the ADEA.[************]

5. Civil Rights Act of 1866

Although the Civil Rights Act of 1866, 42 U.S.C. § 1981 ("Section 1981") does not address document retention, the parallel evidentiary burdens of Title VII and Section 1981 should encourage employers to comply with the document retention requirements articulated by the EEOC in order to avoid adverse inferences or other harmful rulings and consequences in a Section 1981 action.

6. Americans with Disabilities Act ("ADA")

The PWI retention requirements of the ADA mirror the Title VII requirements.

7. Employee Retirement and Insurance Security Act ("ERISA")

The "recordkeeping" requirements of ERISA do contemplate ESI, but also display a wariness about information stored electronically. As with most legal retention schemes, the ERISA regulations require the preservation of information and acknowledge the electronic storage option rather than mandate an electronic form.[††††††††††††] Sections 107 and 209 of ERISA contain certain requirements relating to the maintenance of records for reporting and disclosure purposes and for determining the pension benefits to which participants and beneficiaries are or may become entitled. The record maintenance and retention requirements of ERISA with electronic media if:

- the "electronic recordkeeping system has reasonable controls to ensure the integrity, accuracy, authenticity and reliability of the records";

[************] 29 C.F.R. § 1625 et. seq. ; 29 CFR 1627.2
[††††††††††††] 29 C.F.R. § 2520.107-1

- the "electronic records are maintained in reasonable order and in a safe and accessible place, and in such manner as they may be readily inspected or examined" (e.g. capability of "indexing, retaining, preserving, retrieving and reproducing the electronic records");
- the "electronic records are readily convertible into legible and readable paper copy"; and
- "[a]dequate records management practices are established and implemented" (e.g., "procedures for labeling of electronically maintained or retained records, providing a secure storage environment, creating back-up electronic copies and selecting an off-site storage location, observing a quality assurance program evidenced by regular evaluations of the electronic recordkeeping system including periodic checks of electronically maintained or retained records").[‡‡‡‡‡‡‡‡‡‡‡‡]

Like many other retention laws, the ERISA regulations focus on the legibility of the information when viewed via some electronic transmission (e.g. computer monitor). Electronic records must

> exhibit a high degree of legibility and readability when displayed on a video display terminal or other method of electronic transmission and when reproduced in paper form. The term ``legibility'' means the observer must be able to identify all letters and numerals positively and quickly to the exclusion of all other letters or numerals. The term ``readability'' means that the observer must be able to recognize a group of letters or numerals as words or complete numbers.[§§§§§§§§§§§§]

The regulations permit the substitution of ESI for paper documents but only if the resulting electronic record would "constitute a

---

‡‡‡‡‡‡‡‡‡‡‡‡ Id.
§§§§§§§§§§§§ Id.

duplicate or substitute record under the terms of the plan and applicable federal or state law.”[*]

8. Occupational Safety and Health Act (OSHA)

OSHA requires employers to record occupational accidents and illnesses and to collect and compile occupational safety and health.[†] Most information must be retained for 5 years after the end of the year to which the information relates.[‡] OSHA’s reporting schemes do not discuss ESI. For example, the employer must “orally” report a workplace death within 8 hours after the occurrence by telephoning the nearest OSHA office or using the agency’s 800 number.[§]

9. OFCCP-Executive Orders

“Record retention” requirements under the OFCCP require contractors with 150 or more employees and a contract greater than or equal to $150,00 to maintain for 2 year “any personnel or employment record” including records relating to

> hiring, assignment, promotion, demotion, transfer, lay off or termination, rates of pay or other terms of compensation, and selection for training or apprenticeship, and other records having to do with requests for reasonable accommodation, the results of any physical examination, job advertisements and postings, applications and resumes, tests and test results, and interview notes [and any employment termination].[**]

---

[*] Id.

[†] 29 C.F.R. § 1904.4 through 1904.11.

[‡] Records of “serious adverse reactions” must be kept for 30 years. Toxic Substances Control Act, 15 U.S.C.A. § 2601 et seq.

[§] 29 C.F.R. § 1904.39.

[**] 41 C.F.R. § 60-1.12. The Davis-Bacon and Copeland Act also impose record requirements on contractors and subcontractors performing federally funded or assisted contracts in excess of $2,000 for the construction, alteration, or repair (including painting and decorating) of public buildings or public works. 29 C.F.R. Parts 4 and 5.

Contractors employing less than 150 employees or having a contract less than $150,000 need keep the same “records” for only one year. Affirmative action plans and related documentation must be maintained for the immediately preceding year. The OFCCP regulations specifically call for an adverse inference against any contractor that fails to preserve the required records.[††††††††††††††]

10. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPPA, in part, expanded the healthcare protection of group health plans and imposed a scheme to assure the privacy of personal healthcare information. Employers are required to retain certificates of coverage and other coverage PWI. F “Covered entities” subject to HIPAA’s privacy scheme must develop HIPAA compliance policies and procedures and retain all required documentation for 6 years from the date of its creation or the date when it last was in effect, whichever is later.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡]

HIPPA does contemplate that information will be stored in electronic form. For example, a covered entity must “maintain a written or electronic record” of any “action, activity, or designation [required] to be documented.[§§§§§§§§§§§§§§]

11. Sarbanes-Oxley Act of 2002

Enacted July 30, 2002, the Sarbanes-Oxley Act of 2002 imposes on publicly traded corporations and their professional advisors a variety of auditing systems and controls in order to deter corporate fraud and corruption.[**************] As directed by Sarbanes, the SEC issued rules requiring each reporting company to disclose in its annual report whether a written ethics code governs the company’s principal executive officer, principal financial officer, principal accounting officer or controller, or

---

[††††††††††††††] 41 CFR § 60-1.12

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡] 45 C.F.R. § 164.530.

[§§§§§§§§§§§§§§] Id.

[**************] 12 U.S.C. § 1831m.

persons performing similar functions.[†††††††††††††††] In effect, the requirement called for all covered companies to develop and adhere to an ethics policy.

Sarbane's accounting, reporting, and ethics-code requirements called for extensive recordkeeping functions.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] In implementing the record-keeping requirement, Sarbanes incorporates electronic recordkeeping and reporting schemes.

12. The Immigration Reform and Control Act of 1986 (IRCA)

The Immigration Reform and Control Act (IRCA) requires employers to obtain identity and work authorization information from new and existing employees and to record the information in the federal Form I-9.[§§§§§§§§§§§§§§§] I-9 forms must be retained by "an employer or a recruiter or referrer for a fee" and kept (a) in the case of an employer, for three years after the date of the hire or one year after the termination of employment, whichever is later; or (b) in the case of a recruiter or referrer for a fee, three years after the date of the hire.[***************] Returning employees need not be re-verified if the return occurs within three years after completion of an I-9 form.[†††††††††††††††]

To verify identity and work authorization, an employee must present certain statutorily identified documents. An employer, or a recruiter or referrer for a fee may, but is not required to, copy the document(s) presented by an individual to comply with the verification

---

[†††††††††††††††] 17 CFR" 249.220f. 249. 240f and 249.308; 18 U.S.C.A. §1520(a)(1)(2)..

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] The SEC regulations, which apply to audits or reviews completed on or after October 31, 2003, establish a seven-year retention period for "records relevant to the audit or review, including workpapers and other documents that form the basis of the audit or review, and memoranda, correspondence, communications, other documents, and records (including electronic records), which (1) are created, sent or received in connection with the audit or review, and (2) contain conclusions, opinions, analyses, or financial data related to the audit or review." 17 C.F.R. § 210.2-06(a).

[§§§§§§§§§§§§§§§] 8 U.S.C.A. § 1101; C.F.R. § 274 a.2(2)

[***************] 8 C.F.R. § 274(a)

[†††††††††††††††] 8 C.F.R. § 274.

requirements.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] If an employer does copy the document(s), the documents must be retained with the Form I-9. The regulations provide that the "retention requirements in [regarding Form i-9] do not apply to the photocopies.

IRCA does not address electronic preservation of I-9 forms or supporting information. IRCA does permit the use of microfilm and imposes on the employer the duty to provide the necessary readers during an investigation.[§§§§§§§§§§§§§§§§] Employers electronically storing I-9 forms and information should expect to provide all necessary hardware and software to enable a federal investigator to review the I-9 form and any other stored information.

13. Employee Polygraph Protection Act

The Employee Polygraph Protection Act (EPPA) and related regulations prohibit an employer from conducting polygraph examinations of employees except in very limited circumstances. The EPPA requires an employer to maintain the following PWI: opinions, reports, charts, written questions, lists, and other records relating to polygraph tests of such persons. Neither the EPPA nor its regulations discuss electronically stored information (ESI).[*****************]

14. Federal Withholding, Unemployment, and Social Security Requirements

The Federal Insurance Contribution Act (FICA), the Federal Unemployment Tax (FUTA) and Federal Income Tax Withholding regulations require employee records related to mandatory federal taxes to be retained for at least four years from the due date of a tax or the date of withholding.[††††††††††††††††] These records include basic employee demographic records (such as name, address, social security number, gender,

---

‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡ 8 C.F.R. § 274 a.2(3).
§§§§§§§§§§§§§§§§ 8 C.F.R. § 274 a.(2)(B)(iii)
***************** 41 C.F.R.§ 801.30
†††††††††††††††† 26 C.F.R. § 1.1 et seq.

date of birth, occupation and job classification) along with records of total compensation, tax forms, records of hours worked (straight time and overtime), and payments to annuity, pension, accident, health, or other fringe benefit plans, as well as all wages subject to withholding and the actual taxes withheld from wages.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] IRS tax and compensation directives specifically address electronic reporting and recordkeeping.[§§§§§§§§§§§§§§§§§]

15. Fair and Accurate Credit Transactions Act (FACTA)

Enacted to protect consumer and company privacy, the Fair and Accurate Credit Transactions Act (FACTA) requires every employer to dispose of “consumer information”, i.e., “any record about an individual, whether in paper, electronic, or otherwise, that is a consumer report or is derived from a consumer report” as defined by the Fair Credit Reporting Act, 15 U.S.C. 1681 et seq.[*****************] Assuming the specific provision of FACTA would trump the more general requirements of older retention laws, an employer possessing consumer information about an employee must dispose of the information in a manner that preserves the confidential nature of the information.[†††††††††††††††††]

16. Spoliation

The proliferation of ESI has increased the potential for litigation gamesmanship. Responding to the borderline tactics of some counsel and the flagrant destruction of documents by some parties, courts and legislature have responded with “spoliation” rules and guidelines containing consequences for acts of interference with the production of relevant evidence.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] Castigating parties

---

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] Id.

[§§§§§§§§§§§§§§§§§] 26 C.F.R. § 1.1 et. seq.

[*****************] 16 C.F.R. § 682.1.

[†††††††††††††††††] 16 C.F.R. § 682.3. FACTA requires disposal of records that appear to be required by other retention laws. For example, both Title VII and the ADEA require retention of information that bears on hiring and other employment decisions.

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] Thompson v. Unites States Dep’t of Hous. & Urban Dev., 219 F.R.D. 93 (D. Md. 2003)(court barred the introduction of over 80,000 email discovered during the last minute); .

who hide evidence has long been a part of our system of justice. Courts have not been reluctant to impose adverse inference and other sanctions for the destruction or hiding of evidence. "[T]he rule is that every inference is to be drawn against a party to a suit guilty of mutilating documentary evidence. Gorham v. Montfort, 137 Ga. 134; 72 S.E. 893 (1911) citing Hayes v. Davis, 82 Mo. 209; 1 Starkie on Evid. (3d ed.) 564; 1 Wigmore on Evid. 278.

For PWI retention systems, the concepts of legal spoliation provide strong incentives to develop information retention programs that avoid an unintended loss of information. The costs of litigation should encourage business to consider deploying a retention program that can respond and quickly mesh with the process of litigation.

17. 2005 Proposed E-Amendments to the FRCP

PWI retention requirements for employers will be significantly affected if the Supreme Court implements the proposed amendments to the Federal Rules of Civil Procedure set forth in the 2005 FRCP Report. Responding to growing tension between rules of discovery and ESI, the Advisory Committee on Civil Rules[§§§§§§§§§§§§§§§§§§] undertook a review of the Federal Rules of Civil Procedure "to determine whether changes can be effected to reduce the costs of discovery, to increase its efficiency, to increase uniformity of practice, and to encourage the judiciary to participate more actively in case management."[*******************] If implemented, the changes to the discovery rules will directly affect an employer's creation, preservation, and management of PWI.

[§§§§§§§§§§§§§§§§§§] 2005 FRCP Report, § I.C.1. On May 27, 2005, the Standing Committee on Rules of Practice and Procedure adopted the report developed and submitted by the Advisory Committee on Civil Rules. The Committee will transmit the proposed new rules and amendments to the Judicial Conference at its September 2005 session with recommendations that the rules and amendments be approved and transmitted to the Supreme Court. If finally approved by the Supreme Court, the proposed amendments could become effective as early as December 2006.

[*******************] 2005 FRCP Report § I.C.1

Summary of Proposed Amendments. The 2005 FRCP amendments define and adopt "electronically stored information" (ESI) as a separate category of information subject to discovery. The changes address three areas of recognized sources of difficulty in electronic discovery: "the form of producing electronically stored information in discovery; preserving information for the litigation; and the assertion of privilege and work-product protection claims." The electronic Amendments revise Rules 16, 26, 33, 34, 37 and 45, and Form 35.

Changes to Rules 16 and 26 focus on early identification of potentially discoverable sources of ESI and related discovery issues. The proposals amend Rule 26(f) to require parties to discuss ESI during the mandated discovery-planning conference.[†] The parties would be directed to "develop a proposed discovery plan that indicates the parties' views and proposals" regarding discovery of ESI. This early discovery conference should address production problems, preservation requirements, and treatment of privileges and trial preparation materials.[‡] Any discovery agreement would be placed in the parties' Form 35 report to

[†] Proposed Rule 26(f) amendments:

(f) Conference of Parties; Planning for Discovery. … [T]he parties must [meet] … , to discuss any issues relating to preserving discoverable information, and to develop a proposed discovery plan that indicates the parties' views and proposals concerning:

…

(3) any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced;

(4) any issues relating to claims of privilege or protection as trial-preparation material, including – if the parties agree on a procedure to assert such claims after production – whether to ask the court to include their agreement in an order;

[‡] "One concern initially raised about adding electronically stored information to Rule 26(a)(1) was that it could require parties to locate and review such information too early in the case. … The disclosure obligation has been read as applying to electronically stored information and will continue to apply. The obligation does not force a premature search, but only requires disclosure, either initially or by way of supplementation, of information that the disclosing party has decided it may use to support its case." 2005 FRCP Report, § I.C.2.i, page 32-33.

the presiding judge who may incorporate the agreement into the Rule 16(b) scheduling order.[§§§§§§§§§§§§§§§§§§§§]

ESI – A New Discovery Category. Although electronic “data compilations” have been addressed in FRCP since 1970, the Rules Committee concluded that ESI should be treated as a separate category from “documents.” The Committee recognized that ESI differs from paper documents.

> The most salient of these differences are that electronically stored information is retained in exponentially greater volume than hard-copy documents; electronically stored information is dynamic, rather than static; and electronically stored information may be incomprehensible when separated from the system that created it.[********************]

To accommodate the differences between paper documents and ESI and their accompanying challenges unique to each category, the Rules Committee distinguished ESI from documents.[††††††††††††††††††††]

[§§§§§§§§§§§§§§§§§§§§] Proposed Rule 16(b) amendments:

(b) Scheduling and Planning. …

The scheduling order may also include

…

<u>(5) provisions for disclosure or discovery of electronically stored information;</u>

<u>(6) any agreements the parties reach for asserting claims of privilege or protection as trial-preparation material after production;</u>

[********************] 2005 Rules Report, § I.C.1.

[††††††††††††††††††††] Proposed Rule 33 (d) amendments continue to allow a party the option of responding to an interrogatory by specifying a “record” from which the answer may be found. The proposed Amendments make clear that a record may be ESI.

Rule 33. Interrogatories to Parties

…

(d) Option to Produce Business Records. Where the answer to an interrogatory may be derived or ascertained from the business records<u>, including electronically stored information</u>,

ESI Identification and Production Requirements. Proposed changes to Rule 26(a)(1)(B) require parties to discuss and to disclose prior to the commencement of discovery electronically stored information as well as documents that it may use to support its claims or defenses.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] "The dynamic nature of electronically stored information, and the fact that routine operation of computer systems change and delete information, makes it important to address preservation issues early in cases involving discovery of such information."[§§§§§§§§§§§§§§§§§§§§§]

The Committee has incorporated into the early discussion a process that distinguishes reasonably accessible ESI from ESI that is not "reasonably accessible to the party that has it."[*********************] Amendments to Rule 26(b)(2)(B) relieves a party from producing ESI identified as not being reasonably accessible "because of undue burden or cost."[†††††††††††††††††††††] In refusing to produce the unreasonably accessible

---

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] Proposed Rule 26(a)(1)(B) amendments:

> (1) Initial Disclosures. Except in categories of proceedings specified in Rule 26(a)(1)(E), or to the extent otherwise stipulated or directed by order, a party must, without awaiting a discovery request, provide to other parties:
>
> …
>
> (B) a copy of, or a description by category and location of, all documents, electronically stored information, ~~data compilations~~, and tangible things that are in the possession, custody, or control of the party and that the disclosing party may use to support its claims or defenses, unless solely for impeachment;

[§§§§§§§§§§§§§§§§§§§§§] 2005 FRCP Report § I.C.2.i.

[*********************] Proposed Rule 26 Committee Note, subdivision (f), 2005 FRCP Report.

[†††††††††††††††††††††] Proposed Rule 26(b)(2)(B) Amendments:

> (b) Discovery Scope and Limits. Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:
>
> …
>
> (B) A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party

ESI, the producing party must identify “by category or type” the “source” believed to contain the potentially discoverable ESI and explain the burdens and costs of providing the information and the likelihood of finding it.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡]

If the requesting party continues to desire production of the ESI, the issue may be brought to the Court either through a motion to compel or motion for protective order.[§§§§§§§§§§§§§§§§§§§§§] The responding party bears the burden of showing that the sources of ESI are not reasonably accessible because of undue burden or cost.[**********************] Even if the responding party satisfies its burden, production of unreasonably accessible ESI, still, may be required if the court finds good cause supports production.[††††††††††††††††††††††] In analyzing good cause, the court will balance the costs and potential benefits of discovery.[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡]

Preserving ESI. The Committee recognizes that electronic information systems routinely modify, overwrite, and delete information.[§§§§§§§§§§§§§§§§§§§§§§] The amendments to Rule 37(f) provide some protection against sanctions where requested ESI has been lost as a result of a “routine operation of an electronic information system [and] that operation is in good faith.”[***********************]

---

shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] Id.

[§§§§§§§§§§§§§§§§§§§§§] Id.

[**********************] Id.

[††††††††††††††††††††††] Id.

[‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡‡] Proposed Rule 26(b)(2)(B) Committee Note; 2005 FRCP Report § I.C.2.ii..

[§§§§§§§§§§§§§§§§§§§§§§] 2005 FRCP Report § I.C.2.v.

[***********************] Id. Proposed Rule 37 (f) amendments provide:

(f) Electronically stored information. Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system; see Proposed Rule 37(f) Committee Note; 2005 FRCP Report § I.C.v

The Committee also recognizes the potential harm caused by the interference or cessation of an information system.

> By contrast, electronic information is usually part of the data producer's activities, whether it is the manufacture of products or the provision of services. It can be difficult to interrupt the routine operation of computer systems to isolate and preserve discrete parts of the information they overwrite, delete, or update on an ongoing basis, without creating problems for the larger system. It is unrealistic to expect parties to stop such routine operation of their computer systems as soon as they anticipate litigation. It is also undesirable; the result would be even greater accumulation of duplicative and irrelevant data that must be reviewed, making discovery more expensive and time-consuming.[†]

With respect to the state of discovery law, the Committee highlights the legal uncertainty regarding a party's duty to "interrupt the operation" of an electronic system "to avoid any loss of information" because some ESI might be discoverable.[‡] Indeed, the Committee acknowledges that "[d]efining the culpability standard that would make a party ineligible for protection under Rule 37(f) presented a challenge."[§] Instead of proposing a rule that permits sanctions for "negligence", or limits sanctions to an "intentional" or "reckless" failure to preserve information, the Committee's proposed Rule 37(f) provides protection from sanctions only when the loss of information is due to a "routine, good-faith operation" of a system.[*]

[†] 2005 FRCP Report § I.C.2.v.

[‡] Id.

[§] Id.

[*] Proposed Rule 37(f) amendments:

(f) Electronically stored information. Absent exceptional circumstances, a court may not impose sanctions under these rules

Although providing a type of safe-harbor from sanctions for loss of ESI, the Committee states that the proposed Amendments do not relieve a party of the common-law and statutory responsibility of preserving relevant information. In response to questions about a party intentionally making ESI inaccessible to circumvent a duty to produce, the Committee reaffirmed that the accessible/non-accessible analysis does not "undermine or reduce common-law or statutory preservation obligations."[†]

The development of the doctrine of spoliation has resulted in the coinage of the phrase "litigation hold", a state in which the routine operation of an information system has been interrupted or stayed in order to avoid destroying relevant information. Rule 37's Committee Note points out that the good faith operation of an information system necessary to avoid sanctions, could, in some circumstances, require a party to impose a litigation hold for information from sources the responding party has identified as inaccessible.[‡]

V. RECOMMENDATIONS

A. PWI Retention Systems

Every employer should implement some type of PWI retention system.[§] Companies that have developed or purchased a

---

<u>on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system</u>.

[†] 2005 FRCP Report § I.C.2.ii.

[‡] Proposed Rule 37(f) Note; 2005 FRCP Report § I.C.v.

[§] Most retention systems include;

1. a description and classification of PWI;
2. a designated length of retention and the destruction of targeted data;
3. steps to implement and monitor the system;
4. selection of a PWI retention person to oversee implementation, monitoring and reporting functions;
5. procedures for deviating from the system;
6. procedures for dealing with confidential and/or privileged documents; and

document retention system should already possess most of the proper methods of handling PWI. Due to the relatively recent creation of document retention systems, most of these systems incorporate management of ESI, but may not have considered the proposed amendments to the FRCP. Thus, large corporations and small employers whose budgets do not permit an elaborate PWI retention system should canvass their PWI and, to the extent possible, incorporate the following PWI retention strategies.

1. Identify All Categories of PWI

Employers through their key employees and human resource professionals should identify categories of PWI and the source(s) of each category. Exclusively HR systems should be distinguished from integrated business systems. In addition, systems containing not reasonably accessible ESI should be distinguished from systems containing accessible data.

2. Identify All Legally Mandated PWI Retention Periods

The law mandates different periods of retention among the categories of PWI. (A chart of PWI retention requirements has been provided in the Appendix and should help identify the retention period applicable to each category of PWI.) Retention distinctions may be made between accessible and inaccessible data consistent with proposed FRCP amendments and applicable spoliation laws.

3. Establish Additional Retention Periods

Categories of PWI not subject to legal retention periods, still, should be destroyed in a considered and prescribed timeframe. Some types of e-mail illustrate the less significant, unregulated PWI that should be subject to a considered and prescribed retention period. A smaller category of unregulated, but fundamental PWI might be retained indefinitely. For example, a company might preserve indefinitely its significant historical communications and transactions, or early product or service developments.

---

7. regular audits and reviews of the system.

See sections IV.A.18, *infra*.

4. Routinely Destroy PWI

Consistent with schedules of a PWI retention system, PWI should be routinely destroyed. The proposed amendments to FRCP provide some legal protection for the destruction of PWI during a "routine operation." The proposed amendments' treatment of a routine operation encourages the use of the words as well as the practice in a PWI retention system.[†] In addition to increasing costs, adding to unproductive physical and electronic space, and creating confusion, failing to destroy PWI could needlessly trigger enormous and expensive searches for information requested during discovery; or worse, result in the disclosure of harmful information not legally required to be produced.

5. Include All Sources of PWI

A retention system should expressly apply to all sources of PWI.[‡] For example, PWI stored on a personal computer of telecommuting employees should be covered by the retention scheme as well as the hard-drives of local personal computers, network servers, laptops, PDAs, and backup systems. The 2005 FRCP Report's incorporation of the accessibility of "sources" as a criterion in determining unreasonably accessible ESI should encourage employers to identify both ESI and paper sources of PWI.

6. Suspend Routine Destruction for Potential Litigation

Consistent with the recommendations of sections V. B. and V.C. below, a company should suspend destruction of PWI after becoming

---

[†] The function of destroying PWI can be a complicated process. How to destroy a harddrive or a website located on a remote ISP often requires professional, IT assistance, at least in the formulation of a destruction plan. Destruction of PWI also carries the need to protect confidential information and comply with other legal mandates. Thus, general or outside counsel should be involved in the formulation stage.

[‡] See section III.B., supra. As discussed above, accessibility, "form", and the presence of "alternative" sources may affect the legal retention requirements. Sec section IV.A.18, supra

aware of actual or potential litigation. A process for suspending destruction of PWI ("litigation hold") should be developed or, at least, considered before encountering a real need for a litigation hold. After becoming aware of actual or anticipated litigation, both legal and non-legal representatives of the company should identify all records related to Akey players@ and all other categories of records most likely to be discoverable in the litigation. These documents should be preserved in accessible form to avoid the cost of restoration and retrieval from backup tapes. Akey players@ should be instructed concerning the types of newly created documents that must be preserved. Counsel, with the assistance of IT personnel, should identify all forms of backup storage potentially containing relevant evidence. If the business can identify backup tapes that might contain discoverable evidence not available elsewhere, those tapes should be excluded from routine recycling. Doubt concerning whether to retain or destroy certain documents should be resolved in favor of preservation.

B. Investigations

Most federal retention laws and regulations provide an enforcement scheme and permit federal investigations. If subject to a PWI investigation, employers should review the related enabling laws or regulations for the scope of PWI sources. For some investigations, the duty to preserve a document may be limited to paper records. Other investigations may extend to a review of ESI and all of the various sources of ESI. Although some laws identify the source of PWI sought in an investigation, most investigations begin without any specification of the source. In such situations, employers should review the available sources of PWI and the possible results of the investigation before making PWI available to outside investigators.

The discovery production scheme proposed by the 2005 FRCP Report might be used by a company to justify limiting the response to an expansive investigatory request for PWI.[§§§§§§§§§§§§§§§§§§§§§§§§§] A company may conclude that reviewing all PWI potentially targeted in an investigation may

[§§§§§§§§§§§§§§§§§§§§§§§§§] See section V.C., infra.

be impractical due to the cost or accessibility. Using the proposed discovery scheme as a decision-tree, a party faced with an expansive investigation might first determine whether the PWI potentially requested in an investigation is preserved in a source not reasonably accessible? If so, can the company produce alternatives to inaccessible PWI? If the potentially sought PWI is located in a reasonably accessible source, can the investigation be limited to a primary source of PWI and not all of the underlying source data?

In addition to defining the scope of the investigation, a company should also determine whether the employer bears the legal responsibility for providing the hardware and software necessary to review the stored PWI. A few investigatory schemes require the employer to provide the apparatus necessary to review the information; most federal schemes do not provide such direction. Even for investigations that do require an employer to provide the necessary hardware and software, employers should consider providing the necessary computers, applications, monitors, etc. Most federal and state PWI retention schemes permit the use of subpoena to carry out the statutory purposes. An investigator that resorts to subpoena may be able to convince a reviewing court that the employer is intentionally stalling and to obtain from the court a subpoena with requirements more draconian than simply providing viewing equipment.

Companies faced with an investigation should consider whether the known circumstances justify a litigation hold. Regularly scheduled investigations or reviews such as the annual audits of banks should not reasonably provide notice of a potential legal dispute. Some investigations may be commenced by a disgruntled employee as in a charge of discrimination filed with the EEOC and would justify a litigation hold. Other investigations may be the result of either a randomly or regularly scheduled investigation or a response to allegedly wrongful conduct; e.g. a wage and hour investigation could be initiated by a class of employees seeking overtime or by a random selection of a company within a target industry. To the extent possible, a company must determine the underlying cause of any federal investigation seeking PWI.

C. Litigation Responses

The proposed amendments to FRCP require counsel to discuss potential uses, needs, and issues of ESI; to produce reasonably accessible ESI; and to identify sources of ESI not reasonably accessible. The mandatory early discovery functions impose on counsel an unstated duty to undertake an early analysis of every case and discuss the analysis with the client. To help a client understand the role a party plays in litigation, the early litigation client meeting should include:

1. an explanation of all potential claims and defenses and the related elements of each claim and defense;
2. an explanation of the discovery process and the court's role in managing the process including the concept of adverse inference and sanctions;
3. identification of any potentially relevant evidence including the party's PWI including ESI; and the sources of PWI;
4. an understanding of the party's routine operation of its PWI retention system (include IT personnel);
5. a determination of reasonably accessible and not reasonably accessible ESI;
6. a direction to the party and "key players"[*]:
   - to produce all relevant PWI including ESI;
   - to preserve all discoverable PWI;
7. resolution of how destruction of extant and future ESI will be managed.

The process of overseeing the destruction of extant or future ESI Finally, the attorney and client must decide who will decide whether information may be destroyed. To have litigation counsel review all ESI or every source of ESI would be impractical both in terms of cost and reliability. On the other hand, giving a client unbridled freedom to destroy information risks the most extreme sanctions for spoliation.

[*] Zubulake v. UBS Warburg, 217 F.R.D. 309 (S.D.N.Y. 2004), - A company discovery responsibilities extend to information within the possession of "key players"

The proposed amendments offer guidelines to help determine who should serve as the information-destruction gatekeeper. A client must understand the importance of identifying inaccessible sources of ESI early in litigation and administering its information systems in a good faith and routine manner, including ESI retirement and destruction programs. Although extreme circumstances could support a Court ordering the production of ESI located in an inaccessible source, a party's early and diligent compliance with the proposed E-rules and a good faith, routine operation of the PWI management program should prevent a court from sanctioning the party for the loss of ESI.

VI. CONCLUSION

Employers attempting to develop a PWI retention strategy that satisfies both basic business objectives and the law may encounter a moving target. For most businesses, a competitive product or service requires the use of some technology. For many categories of PWI subject to legal retention requirements, the incorporation of the new technology adds to the amount of PWI that must be managed. Answering the legal question, " What PWI must be kept and how?" may depend on the date. Have the amendments proposed by the 2005 FRCP Report been adopted? Has the definition of a document retention law been amended or interpreted by a court? Is litigation a reasonable possibility? As the law and business continue to struggle with the evolution of technology, the proposals of the 2005 FRCP Report might offer a transitional approach for business seeking to develop a rational and legal PWI retention system, at least until the law or business offers a clearer solution.

VII. APPENDIX

CHART OF RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Note: The information contained in the following chart attempts to connect a particular category of workplace information with the applicable federal retention requirements. Since many federal retention schemes do not address a particular category of workplace information, the following should not be accepted as an exhaustive analysis, but simply a guide for deeper inquiry including particular state or local retention requirements.

Information Type	Information Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
1. Race, Ethnic Identity: (optional) post-employment record, if permitted by state law.	Not specified	separate from personnel files	permanent	Not specified		29 CFR 1602.13	Information necessary for completion of items 5 & 6 of Report EEO-1
2. Gender Identity: gender based pay records			2 yr			29 CFR 1602.12 29 CFR 1620.32	
3. Age Identity			3 yr			29 CFR 1627.3	

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
4. Veteran identity: number of special disabled vets, Vietnam-era vets, and other protected vets; new employees hired during reporting period at each location; number of special disabled, Vietnam-era, and other protected vets hired.	VETS-100 Report	Not Specified in either 41 CFR or 38 USC 2012	Not Specified in either 41 CFR or 38 USC 2012			41 CFR 61-250.10 38 USC 2012	Applies to Federal Contractors and Subcontractors. VETS-100 reports must be submitted no later than September 30 of each year beginning September 30, 2001.

Irvin, Stanford & Kessler LLP
2005

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
5. Applications, resume, responses to job ads, physical examinations and records pertaining to refusal to hire.	The EEOC has the power trough the ADEA § 626, and Title VII § 790(c) to require production of any document or record they deem necessary consistent with their authority to investigate alleged violations.		1 yr from date of employment termination and 1 year from the making of the record or a personnel action.			ADEA § 626; 29 CFR 1627.3; Title VII §790(c); 29 CFR 1602.14;	Federal contractors see No. 35 below

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
6. Hiring Documents (also rejection documents)	Not specified		1 yr. after date of record creation, or the date of the last personal action. If employee terminated- one year past date of termination. Where a charge of discrimination has been filed or an action taken, records kept until final disposition of the charge or action.			29 CFR 1602.14 29 CFR 1627.3	Federal contractors see No. 35 below

Irvin, Stanford & Kessler LLP
2005

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
7. Position/Job Description	The EEOC has the power trough the ADEA § 626, and Title VII § 790(c) to require production of any document or record they deem necessary consistent with their authority to investigate alleged violations.		1627.3 requires 1 year past the last action taken on the docs.			29 CFR 1627.3 ADEA § 626;	

Irvin, Stanford & Kessler LLP
2005

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
8. Compensation Payroll (name, address, DOB, occupation, weekly compensation); individual contracts, collective bargaining agreements, notices of Wage-Hour Supplemental records- wage rate tables; work time schedules; time sheets, records; order, shipping, billing records; wage addition or deduction records Certificates of Age	Electronic format permitted		3 yrs from last date of pay. 2 yrs from date of last entry. Until end of employment			29 CFR 516.5; Equal Pay Act 29 CFR 1620.32 incorporates 29 CFR 516 29 CFR 1627.3 ADEA- 29 USCS §626 refers back to EEOC at 29 CFR 1627.3 29 CFR 516.6 29.CFR 1620.32	Federal contractors see No. 35 below (Title VII requires 1yr 29 CFR 1602.14)

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
9. Benefits:	Electronic form permitted as replacement for paper documents					29 CFR 1602.14 29 CFR.2520.107-1	Federal contractors see No. 35 below
general (i.e. non-plan)			1 yr				
records providing basis for all required “plan” descriptions or reports			6 yrs after filing date of document/			ERISA 29 USC 1027	
records pertaining to each employee-participant in the plan for determining benefits			as long as relevant				
benefit plans, seniority merit systems			length of plan plus 1 yr			29 CFR 1627.3	

Irvin, Stanford & Kessler LLP
2005

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
10. I-9, Eligibility and Verification documents			1 yr after termination (3 yrs after hiring or recruited or referred for a fee).			IRCA; 8 USC 1324(b)(1)(e)(3)	
11. Investigation: Criminal							I'm not sure what you are getting at here. Investigations insofar as hiring- that would be the 1627.3 rules I think. I need more info to help here.
12. Investigation: Financial							Must destroy personal identifying information.
13. Investigation: Education							"
14. Investigation: Employment History							"

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
16. Medical: Medical condition, history, and examinations	Collected and maintained on separate forms	Kept in separate files			Treated as a confidential record except supervisors and managers informed about necessary restrictions and accommodation requirements	29 CFR 825.500 29 CFR 1627.3 29 CFR 1630.14; 41 CFR 60-250.23	

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
17. Selection *Employers <100 employees:* Records by sex, race, and national origin of persons hired, promoted, and terminated for each job; number of applicants hired, and employees promoted;			Collect information for 2 years after a noted adverse impact is eliminated 29 CFR 1602.14 explains docs must be kept for 1 year past last personnel action.			29 CFR 1607.15A(a) 29 CFR 1602.14	Generally retention time not specified if no adverse impact noted.
selection procedures.			1 yr, and 1 year (Title VII) from any personnel action to which records relate			29 CFR 1627.3	

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
18. Selection *Employers ≥100 employees:* Records for each job showing whether selection process has adverse impact. If adverse impact, records of process component having adverse impact.	EEO-1 reports		Permanently for any period where adverse impact exists plus two years thereafter			29 CFR 1607.15	More than 100 employees must file EEO-1
19. Selection for training or apprenticeship (not apprenticeship records)			1 year from making the record, or 1 year from the date of termination or the final disposition of any discrimination or employment action.			29 CFR 1602.14	

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
20. Leave Records of FMLA compliance, e.g. dates and hours of leave taken, notices, leave policies and benefits, leave disputes	No particular form required but may be kept on microfilm or other basic source document of an automated data processing memory	Place of employment	3 years		Medical records must be kept confidential in files separate from personnel files	29 CFR 825.500	
21. Requests for reasonable accommodation			1 year – less than 150 employees 2 years – 150 employees or more			29 CFR 1602.14; 41 CFR 60-741.80	Federal contractors see No. 35 below
22. Performance			1 year 2 years			29 CFR 1602.14; 41 CFR 60-741.80	Federal contractors see No. 35 below
23. Promotion/ Transfer			1 year 2 years			29 CFR 1602.14; 41 CFR 60-741.80	Federal contractors see No. 35 below
24. Discipline/ Demotion			1 year 2 tears			29 CFR 1602.14; 41 CFR 60-741.80	Federal contractors see No. 35 below

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
25. Lay-off			1 year 2 years			29 CFR 1602.14; 41 CFR 60-741.80	Federal contractors see No. 35 below
26. Termination			1 year – less than 150 employees 2 years – 150 employees or more			29 CFR 1602.14; 41 CFR 60-741.80	Federal contractors see No. 35 below
27. Ethics						Sarbanes	I'm not sure what you are looking for on these next four
28. Executives (CEO, COO, etc)						Sarbanes	‘ ’
29. Board of Directors						Sarbanes	‘ ’

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
30. Temporary (same as for regular employees plus job orders submitted to agencies or unions)			1 yr			ADEA sec. 401; 29 CFR 1627.3	
31. Claims, charges, lawsuit: *Title VII, ADA*, ADEA: Personnel records relevant to charge-includes records of aggrieved person and similarly situated persons	EEOC reserves the right to impose specific record-keeping requirements pertaining to each charge		Until final disposition; i.e. expiration of statute of limitations or termination of litigation, whichever is longer.			29 CFR 1602.12 29 CFR 1602.14; 29 CFR 1627.3; 41 CFR 60-741.80	
32. Required Reports: EEO-1 *Employers ≥ 100 employees*		At reporting unit or headquarters;	A copy of the most recent report filed should be maintained			29 CFR 1602.07	Employers with 100 or more employees

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
33. Required Reports: VETS-100 *Federal contractors ≥ $10,000 contract*			1 yr			38 USC 20012 (d)	
34. Required Reports: AAP and supporting documents of *Federal contractors ≥ $50,000 contract, federal depository, or issuing and paying agent for US savings bonds and notes) with 50 or more employees*			Current and preceding year			41 CFR §60-1.12(b) 41 CFR §60-1.2	

RETAINED WORKPLACE INFORMATION AND RELATED LEGAL REQUIREMENTS

Document Type	Document Form	Retention Location	Length of Retention	Right of Access	Privacy	Source	Comments
35. ***Note***: *Personnel and employment record of federal contractor with ≥150 employees and $150,000 contract*			2 yrs from date of record or personnel action, whichever longer			41 CFR 60-1.12(a)	