Legal Obstacles to E-Mail Message Destruction

The
ARMA International Educational Foundation
1609 Terrie Drive
Pittsburgh PA USA 15241
www.armaedfoundation.org

A Study by

John C. Montaña, J.D.,

with editorial assistance from

John R. Kain, M.A.

and research assistance from

John R. Kain, M.A. and Kathleen Nolan, M.D., M.S.L.

October 19, 2003

Legal Obstacles to E-Mail Message Destruction

A Study by John C. Montaña
For
The ARMA International Education Foundation

Legal Obstacles to E-Mail Message Destruction

1. Introduction

Since the early 1990's e-mail has become as ubiquitous as the computers needed to transmit and receive it. Many businesses are dependent on it, and a good percentage of all private individuals in the developed world are equally dependent on it as a means -- often a primary means -- of communication with others. Nor is this trend limited to the so-called "developed" countries. Anyplace you can find an electrical outlet and a phone outlet, you are likely to find computers and e-mail.

For many years, however, e-mail's acceptance in the world at large outpaced the legal world's ability to deal with it. Change is rapid in the computer world -- In 1965, Gordon Moore predicted that computer capability would double every 18 months, and this prediction has held true. As computer capability and those aspects of it needed to support the use of e-mail -- inexpensive data storage, faster data processing and faster transmission -- have doubled and redoubled, so too has our use and dependence upon e-mail. Large commercial organizations send and receive millions of e-mails every year.

Change comes less rapidly in the legal world, however. Legal processes are by their nature slow: legislation must go through a torturous process of introduction and drafting, amendment and redrafting, negotiations, hearings, debate, compromise and revision, as the implications of the contemplated law are carefully thought through and interested parties weigh in. This may take several years from start to final legislation, and still more years as the law goes through revision to a mature and fully functional rule. Law created by way of case decision in the courts develops even more slowly as an issue wends its tedious way up and down the appellate process, and slowly spreads from jurisdiction to jurisdiction. Case by case, like the bricks of a large and complex house, the judicial doctrine develops over time, in a process that takes years, and often decades.

Nor do the legal systems of the world come to the issue of advanced information technology particularly well suited to deal with it in the first place. The common law legal system of the English speaking world dates from before the first millennium, and the civil law system used by most of the rest of the world is as old -- the so-called "Napoleonic Code" spread around the world by the French emperor of that name is really a modernized (if that is the proper word for a legal code that is now nearly 200 years old) version of the Justinian Code, named for the Roman emperor who appointed a commission in 528 C.E. to gather together Roman law into a single, unified body of statutes and principles.

Given their ages, even paper documents are something of a new-fangled invention for both of these systems, and both devote a good deal of time and effort to overcoming inherent prejudices against written documents and attempting to deal with their supposed unreliability. During the decades that usage of computer systems in commercial environments became widespread, both legal systems operated on an underlying assumption that records were created and maintained on

paper or at least paper analogues such as microfilm;[1] and requirements designed to enhance reliability were imposed upon them that not only presumed the existence of paper, but which were both meaningless and impossible to apply in the context of something as insubstantial as an electronic record. One such requirement that is still commonly found in civil code compilations is the requirement that commercial accounting records be maintained in bound and paginated books which have been authenticated by a notary or other public official.[2]

Such prejudices and requirements impose difficulties on the use of even highly structured electronic records such as accounting software. Something such as e-mail -- by its nature unstructured and unmanaged -- poses a formidable conundrum for the legal systems of the world. The pervasive use of e-mail has occurred pretty much without regard to the legal niceties – if some process offers the possibilities of new market opportunities, increased profits or other commercial advantage, people tend to do business first and worry about legalities later. In the case of electronic documents generally, this is precisely what has happened. In such cases, lawmaking often consists of ex post facto ratifications of practices that have long since become imbedded in the commercial and popular culture.

For structured information such as accounting databases, workarounds which pay at least lip service to paper-based legal requirements are possible -- paper printouts can be substituted for bound volumes,[3] and computer disks and other electronic media can be "authenticated" in an analogue of the numbering and stamping of bound volumes.[4] In the case of e-mail, such workarounds are not viable, even when, as is often the case, the workaround is a legal fiction. E-mail's viability as a legally recognized phenomenon developed against this backdrop, and both legislators and courts were forced to deal with that backdrop as they attempted to decide just what sort of beast e-mail is.

1.1. The Issue

E-mail's convenience and resulting pervasive use means that most organizations are maintaining large volumes of it, notwithstanding the legal issues mentioned above. This poses several problems:

- Even with the continuing drop in prices for electronic storage, continued storage of large volumes of e-mail imposes significant costs on an organization;
- The administrative issues of managing millions or billions of very informal data objects, created with little or no attention to formal structuring or indexing, make systematic recovery of them challenging and expensive;

[1] Itself an invention that required an assortment of statutes and case decisions in many jurisdictions over decades to authorize its legal acceptance -- e.g., although microfilming had been in widespread use world-wide for several decades, Portugal finally authorized its use for commercial records only in the mid-1970's.

[2] *See, e.g.,* Mexico Art. 34, Commercial Code, Republic of China (Taiwan) Income Tax Law Art. 14, Argentina Commercial Code Art 53, Spain Commercial Code Art. 36.

[3] E.g., Greece Books and Records Code prior to its 2002 modifications.

[4] E.g., Greece Books and Records Code Art. 24.

- The e-mail so stored is subject to legal process, requiring searches that may prove very difficult and expensive.

These issues have therefore made the question of e-mail retention one of the cutting-edge issues in information management and risk management. Two general philosophical approaches to dealing with it have emerged:

- *The blanket cut-off.* In this approach, all e-mail is retained for some period -- 60 days, 90 days, 1 year, etc. -- and then deleted *en mass*.
- *The e-mail-as-a-record approach.* In this approach, each e-mail is categorized by subject matter, and given a retention period based upon that subject matter, presumably the same one as other data objects containing similar subject matter.

Each of these approaches has advantages and disadvantages: The blanket approach has the virtues of simplicity and ease of implementation, but assumes -- not necessarily correctly -- that e-mail is homogeneous from both business management and legal perspectives, and all e-mail can therefore be treated identically.

The e-mail-as-a-record approach has the virtues of precision and specificity; and of searchability -- e-mail is retained based upon its assessed value, and is (in theory) recoverable on demand, based upon the categorization given it. The disadvantage of this approach is that categorization of e-mail has proven to be a formidable challenge, to say the least.

1.2. This Project

This project seeks to examine e-mail and the legal doctrines around it, to determine which approach to its retention is the sounder. More precisely it seeks:

> "To identify the legal and statutory obstacles which would prevent the adoption of an information management policy requiring the automatic and systematic deletion of all e-mail messages, in all repositories, older than a predefined period."[5]

The short answer to this question is a simple one: e-mail cannot be destroyed *en mass* after an arbitrarily assigned period in any case where a legal duty requires otherwise. The devil is, however, in the details: Legal duties arise from a great variety of sources, and the duties themselves vary quite considerably. Each such duty creates in the data object upon which it is imposed some sort of legal status -- it is an evidentiary object, a regulatory compliance object, a government record, or whatever. The question then is what, if any, status does the law impose upon e-mail?

That e-mail has *some* sort of legal status is beyond peradventure – for years, e-mail has been a commonly used mode of commercial communication, and this fact by itself guarantees some sort of legal determination as to the significance to the e-mail so used. Negotiations, offers,

[5] AIEF (ARMA International Educational Foundation) RP2003-1 *E-Mail Management Policy,* para. 1.

acceptances, contract terms, legal documents, revisions, disagreements – all the stuff of commercial transactions – have all been transmitted and received via e-mail, and all of these things themselves have legal significance. This document is itself a product of such a process and so is illustrative of it – the process by which it was envisioned, negotiated, drafted, reviewed and finalized consisted almost entirely of phone calls, e-mails and attachments to e-mails. The only hard copy that has ever existed is that which you the reader are now holding – unless of course, you are reading an electronic copy, that you may well have purchased and received via e-mail.

In the larger world, contracts lead to disputes, and disputes lead to court; and if e-mail has been used in the contract process, it too will go to court, even if only to be declared a nullity upon arrival. The question in the case of e-mail is therefore "What exactly is its status, and how does it affect retention practices?" Is e-mail a "written" document, entitled to the same legal status -- and thereby to whatever presumption of reliability and trustworthiness attaches thereto, and any associated duties -- as a paper document? Is it more like a phone call, with its commensurately lower indicia of reliability, and lesser compliment of duties? Or is it more like the oral amendments that often follow written contracts containing a prohibition on oral amendments – a legal non-entity, and completely unenforceable? Given the degree to which business, private individuals and government have been relying on e-mail for the transaction of legally significant matters, this is a vexing and important question.

This paper seeks to clarify that. Fifteen or so years of widespread e-mail use have provided plenty of grist for the legal mill[6], and enough time to grind it. In this document we will examine the current state of the law, attempt to arrive at a reasoned judgment as to what it means insofar as it addresses the status of e-mail as a legally defined object, and then decide whether that status impacts its retention.

1.3. The Concept of Legal Status

The concept of 'legal status" is a misnomer. E-mail, like anything that can be characterized as a 'communication' or 'document' does not obtain a single legal status defining it and authorizing it for all purposes in all jurisdictions. Rather, e-mail is authorized, ratified or otherwise classified by case decision, statute, regulation or other legal authority for a particular purpose, dependent on the legal situation presented, the proposed use of the e-mail, the authority -- court, legislator or regulator -- that is in control, the forum in question, the jurisdiction in which the question is presented and the legal system governing that jurisdiction. E-mail may therefore have some defined status in several subject areas, and that status may well vary from jurisdiction to jurisdiction. At least the following areas present themselves:

The Evidentiary Value of E-mail. The potential utility of e-mail in litigation prompted perhaps the earliest contemplation of its legal status. As in any other communication, people make statements in e-mail. Regardless of the "written" or "authorized" or any other status of an e-mail,

[6] In the form of the aforesaid negotiations, offers, acceptances, contract terms, legal documents, revisions, and disagreements, as well as the misunderstandings, disagreements, misrepresentations and occasional outright lies, frauds and felonies which constitute the fertile soil upon which legal doctrine grows.

those statements often prove interesting and potentially valuable as evidence to the opponent in litigation. This being the case, it is natural that litigants would soon seek to obtain e-mail's admission into court cases, and to develop legal theories that would permit this.

Status as a Document When a "Written" Document is Required. The law in most jurisdictions requires many written documents or records to be maintained by those under its authority. For a long time after its recognition of writing and written documents, the law presumed that "written" meant written on paper. This presumption matched the facts quite nicely for a long period of time. There were, in the final analysis, only two types of communication -- "written" as written on a piece of paper, and aural -- in-person conversations, and later, telephone calls and the like. Notwithstanding that it took time for formal legal acceptance to make the rounds through the many jurisdictions of the world, microfilm posed no theoretical challenge to this. A microfilm is simply a picture of a piece of paper, on a medium very similar with respect to durability and perceived resistance to tampering. More problematic were such things as telegraph or telex messages. A telegraph message poses some of the same theoretical issues as does e-mail – electronic transmission, followed by a capture and transcription process, with whatever uncertainties that entails.

Status as a Properly Maintained Record When a Record is Required. In similar manner, "record" for a very long time meant data recorded on a piece of paper, often a piece of paper bound into a book and authenticated by a public official of some sort. The advent of computers changed that -- electronic accounting systems very rapidly replaced manual systems in large businesses, and soon a large percentage of other records were also being computer-generated. Like it or not, legal authorities had to deal with the presence of electronically generated records.

Status as a Signed Document. Not only does the law often require that there be a written record of something, it often requires that the record be signed to be valid or enforceable. "Signed" is generally taken to mean manually signed, as with a pen. This is not true, as we shall see, and the fact that it is not has proven important in the development of e-mail law.

In each of these areas, law may be made by any of a number of sources, or a combination of them. And, the law so made may be either sweeping and general, or very narrow, and covering only a single situation or usage, or anything in between. In considering e-mail's legal treatment, these sources, and variances in terminology, authority or conceptualization that they bring to the subject, should be borne in mind.

1.4. Common Law versus Civil Law

The scope and sources of law are somewhat different vis-à-vis common law and civil law. In common law jurisdictions, absence of a statutory enactment on a topic does not equate to an absence of law: courts can make law in the absence of a statute on the subject; if there is one, the courts construe it and apply it to particular facts. In both cases, the law so made is as binding and enforceable as any other law; in addition, the common law principle of *stare decisis*, or binding precedent, applies – subsequent decisions by courts within the jurisdiction must be decided in conformance with the rule of law articulated. Over time, a body of decisional law on a topic

builds up, explaining nuances and covering a variety of fact situations. It is not uncommon for an entire and mature legal doctrine to develop in the entire absence of statutory law on the subject. This decisional law – very important in the development of e-mail law -- is common law.

In civil law jurisdictions, courts are much less influential. Courts decide cases by applying statutory law to particular facts, but they are not empowered to create legal doctrine in the absence of statutory law, nor do their decisions have precedential value. Thus, they are far less influential in the development of the law than are the courts of the common law countries.

1.5. Primary and Supplemental Law

In both common law and civil law jurisdictions, primary law – statutes[7] and/or case decisions – are supplemented by other binding legal pronouncements. These are regulations, promulgated by government agencies or pursuant to a grant of authority to run some regulatory scheme, or by the executive, to facilitate the implementation of some law.[8] Regulations are often the legal authorities with the narrowest scope: A regulatory agency has authority to make rules only within the grant of power given it by its governing legislative body, typically within a single subject area or regulatory scheme; therefore, its pronouncements on a topic such as e-mail apply only within the confines of that grant of authority and regulatory arena. Thus, an e-mail regulation may apply only to a limited population of regulated persons or entities, or to a single topical area.

2. E-Mail Defined

When speaking of the legal status of e-mail, the starting point is to define what is meant by the term "e-mail." We tend to think of e-mail as text messages that we send or receive using a specialized computer program such as Outlook, Eudora or Netscape, and directed from one individual human being to another. E-mail is, however, a fuzzy concept, and this conceptualization is not particularly accurate. Everyone who gets e-mail gets a great deal of automated e-mail – advertisements and order acknowledgements are the commonest examples – that cannot meaningfully be said to have a human sender at the other end; and most e-mail users have, at one point or another sent e-mail to an auto-receipt address at a business or government agency that either deals with the response automatically or directs it to some unknown person. Thus, the human-to-human element of e-mail that we often associate with it is clearly not a necessary prerequisite. Such formal definitions as exist do not much tighten the definition or conceptualization. One authoritative definition characterizes it thus:

[7] Statutes from common law countries used in this publication will be variously named as “acts” (e.g.," the Evidence Act”), ordinances or statutes. Civil code statutes are generally referred to by article or section number of a particular code, e.g., Civil Code art 1234.

[8] In common law jurisdictions, they are styled as “administrative regulations”, “regulations”, or “statutory instruments.” In civil law jurisdictions, they are commonly characterized as “decrees”, “decree-laws” or regulations.

> "An electronic means for communication in which (a) usually text is transmitted (but sometimes also graphics and/or audio information), (b) operations include sending, storing, processing, and receiving information, (c) users are allowed to communicate under specified conditions, and (d) messages are held in storage until called for by the addressee. Some e-mail software permits the attachment of separate electronic files, e.g., word-processor files, graphics files, audio files."[9]

This definition places what we normally think of as e-mail in a category with a great deal of other electronic data interchange (EDI). This is not unreasonable. There is no real technological distinction between e-mail and other forms of EDI: the information in the transmission is assembled on a computer, broken into packets, routed over the internet (or an intranet), reassembled on the other end, and made available to the recipient on a computer. What distinguishes these other things from e-mail – to the extent that this can be done – is as much the I-know-it-when-I-see-it factor as anything else.

The legal system itself has had little chance to define e-mail -- by the time it reached the legal system, e-mail had already been defined by technology and usage, and was presented to the legal system as a commonly understood phenomenon from the start. The fuzziness of the concept quickly spilled over into legal definitions. Statutes often avoid any definition of the term entirely. Canada's *Personal Information Protection and Electronic Documents Act*[10] contains a broad authorization of the use of electronic documents and technology, and defines a number of EDI-related terms, but e-mail is not among them. The *Canada Evidence Act* takes a similar tack, defining several terms related to electronic documents, but omitting a definition of e-mail.[11] An example of a very broad definition is found in the Australian Customs Act:

> *"electronic*, in relation to a communication, means the transmission of the communication by computer."[12]

> "For the purposes of this Division, any electronic communication to Customs is taken to be a statement made to the CEO [Customs and Excise Office]."[13]

These two provisions, viewed collectively, clearly contemplate e-mail communication, even though this is not stated. On other occasions, it is referred to simply as "e-mail" or a "data message" without definition:[14]

> "Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference."[15]

---

[9] American National Standards Institute (ANSI), American National Standard for Telecommunications T1.523-2001, Telecom Glossary 2000 (Approved Feb. 28, 2001)
[10] Canada Personal Information Protection and Electronic Documents Act (2000), Part 2.
[11] *See generally, Canada Evidence Act., §§31 to 31.8.*
[12] Australia Customs Act 1901, § 4.
[13] Australia Customs Act 1901, §243W
[14] Except perhaps by reference to another law, for which in this case see 4.4. infra.
[15] United Nations Commission on International Trade (UNICTRAL) Model Law on Electronic Commerce Art. 6 (1) (1996).

or

> "Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the data message purporting to give rise to such legal effect, or that it is merely referred to in that electronic data message."[16]

In each of these examples, the reasoning implicit in the language is that there is a sufficiently strong consensus about what is meant that there is no need to define the term. On the other hand, there is no language in the text that limits the regulated communication to what is normally thought of as "e-mail." Other statutes, while similarly avoiding a formal definition, nonetheless take the step of equating e-mail with letters and other traditional documents.[17]

The United States Archives and Records Administration (NARA), the defendant in a celebrated series of cases defining its responsibilities regarding e-mail and other electronic documents, and a party with a strong incentive to deal forcefully with the issue, takes a similar but slightly more definitive tack in its electronic records management regulations and defines "e-mail message" and "e-mail system" thus:

> *"Electronic mail message.* A document created or received on an electronic mail system including brief notes, more formal or substantive narrative documents, and any attachments, such as word processing and other electronic documents, which may be transmitted with the message."
>
> *"Electronic mail system.* A computer application used to create, receive, and transmit messages and other documents. Excluded from this definition are file transfer utilities (software that transmits files between users but does not retain any transmission data), data systems used to collect and process data that have been organized into data files or data bases on either personal computers or mainframe computers, and word processing documents not transmitted on an e-mail system." [18]

This definition thus *includes* the attachment in the "e-mail," but *excludes* file transfer utilities that do not capture metadata; and internal data transfer within database structures.

Case decisions are similarly postured. The two seminal American case decisions, *Armstrong v. Executive Office of the President*[19] and *Public Citizen v. Carlin*[20] both go through extended analyses of whether e-mail is a public record pursuant to statute, of the proper legal duty of the federal archivist with respect to e-mail, and other matters concerning legal aspects of e-mail without ever defining the object that they have so analyzed. Noteworthy, however, is the *Armstrong* court's observation that e-mail is often indistinguishable from letters and other correspondence with respect to content -- it is, on many occasions, an electronic text version of a letter or memorandum. The court finds this comparison, along with a short description of the

---

[16] Philippines Electronic Commerce Act Art. 6 (2000)
[17] *See, e.g.*, Mexico Commercial Code Art. 49, requiring retention of " letters, telegrams, data messages or any other documents. . . ."
[18] 36 C.F.R. §1234.2
[19] *Armstrong v. Executive Office of the President*, 1 F.3d 1274 (D.C.Cir. 1993).
[20] *Public Citizen v. Carlin*, 184 F.3d 900 (DC Cir., 1999).

characteristics of e-mail -- transmission, receipt and so on -- adequate as a basis upon which to decide the substantive legal issues involved.[21]

The composite created by these authorities that defines "e-mail" is that of a broad class of electronic communication. Based upon both operational and legal definitions, an e-mail can be said to have the following required attributes:

- It is a discrete (as compared to streaming or continuous) electronic transmission;
- of a communication;
- to one or more specific addressees;
- via a computer system or the internet;
- that is captured by the sending and receiving computers; and
- an electronic record of it made and stored.

In addition, the following attributes are commonly associated with e-mail, though not required to place it in the defined class.

- It may be in whole or in part a text message;
- It may have another electronic data object appended to it as an attachment.

This rather vague definition has considerable significance in the analysis of e-mail's legal status – it places e-mail squarely within the purview of a great many laws governing such matters as EDI, electronic business transactions and electronic signatures that do not directly address "e-mail."

3. The Evidentiary Value of E-Mail

Admissibility in court was an early legal forum for e-mail. This is so for two reasons: First, e-mails are often communications between two parties, and such communications are often part of a matter around which a legal dispute arises. The communications are therefore germane to the dispute and one or both of the parties may have an interest in seeing them admitted into evidence. Second, admissibility of any potential evidentiary object is not necessarily tied to its receiving legal sanction as a "record" or some other formally defined or recognized legal object. Use in court therefore did not require waiting for the rest of the law surrounding e-mail to fully develop.

Admissibility in legal proceedings is not a uniform thing – a potential evidentiary object, and in particular an object whose admission is sought because of the meaning of the words it contains, as would often be the case with e-mail -- is not simply "admissible" or "not admissible." Rather, its admissibility may be dependent upon the reason its admission is sought, the rationale behind that admission, and the relationship between the object and the parties in the case. The specifics of those relationships are defined by a variety of statues, court rules, regulations and case decisions that have the potential to vary from jurisdiction to jurisdiction. These authorities are,

[21] *Armstrong v. Executive Office of the President*, at f.n. 4.

in turn, governed by the underlying philosophy of the legal system in which they exist. Within a jurisdiction, there may also be different types of legal actions -- lawsuits, regulatory actions or administrative tribunals -- with differing standards of admissibility.

There are commonalities between law and common law jurisdictions with respect to this, but also some fundamental differences.

3.1. Civil Law Jurisdictions

In civil law jurisdictions, businesses are commonly required by law to maintain a set of business records containing specified records such as ledgers and journals. In addition, they are often required by law to maintain business correspondence sent and received, including e-mail:

> "Merchants shall preserve for ten years the original of letters, telegrams, data messages or any other documents in which contracts are formalized, or which contain covenants or commitments giving rise to contractual rights and obligations."[22]

The requirement to properly maintain records is commonly backed up by a formidable evidentiary incentive:

> "Duly kept accounts[23] may be accepted in the courts in order to act as proof between traders in respect of commercial instruments.
>
> If the accounts have not been duly kept, they may not be invoked by their author for the latter's benefit."[24]

Thus, failure to maintain business records as required by law means that an organization's records can be used in evidence by its opponent, but not by the organization itself. The key to admissibility of an e-mail on one's own behalf is compliance with whatever formalities are required -- if they are not properly maintained, the court is empowered to reject them s evidence in favor of their author, while still possibly admitting them in favor of the author's opponent. In the case of correspondence-like data objects such as e-mail, this may include requirements that correspondence be maintained in chronological order, or be maintained electronically according to specific technical requirements.[25]

Beyond these technical requirements, however, admissibility of a data object such as an e-mail is comparatively simple in civil law jurisdictions. Unlike the common law jurisdictions, with their hearsay rules and other technical requirements for admissibility of evidence (for which see

[22] Mexico Commercial Code Art. 49.
[23] Elsewhere in this codification, the legal requirement to maintain records is extended to required records (i.e., ledgers, journals and other formal accounting documents) and "supporting documents."
[24] France Commercial Code Art. L123-23.
[25] See, e.g., Mexico Commercial Code Art. 49, permitting retention of business correspondence in electronic form provided that the retention meets the requirement of the pertinent technical standard as promulgated in the Normas Officiales Mexicanas (Official Mexican Norms).

below), civil law courts are broadly empowered to receive and consider any evidence that that they feel is necessary for resolution of the dispute before them. Thus, e-mails are used by these courts routinely, in the absence of explicit statutory authorization.[26]

3.2. Common Law Jurisdictions

Common law jurisdictions, by contrast, do not generally impose a flat bar on the admission of any business record merely because its maintenance did not meet a technical requirement. Regardless of the circumstances of its maintenance, it is at least potentially admissible if its probative value is sufficient to overcome any doubts about its veracity. On the other hand, the common law requires any evidentiary object other than live testimony to overcome a series of hurdles prior to its admission into court. These hurdles revolve around the common law hearsay rule.

The Hearsay Rule. At English common law, only live testimony was permitted. Out-of-court statements could not be brought into evidence:

> "Evidence of a previous representation made by a person is not admissible to prove the existence of a fact that the person intended to assert by the representation."[27]

When written documents became germane to legal disputes, they were regarded as recorded out-of-court statements, and therefore hearsay and inadmissible. As litigation has grown more complex, a number of exceptions to the hearsay rule have arisen permitting admission of documentary evidence. Nonetheless, inadmissibility of written documents is the default common law position: " [If a] document is to be admitted as evidence of the truth of the statements it contains, it must be shown to fall within one of the exceptions to the hearsay rule.[28]

Over time, a number of exceptions to the hearsay rule (or definitional solutions defining the exception as non-hearsay) applicable to documents and records have developed by statutory enactment, court rule or case decision. Several are germane to an analysis of e-mail:

Business Records: Variously styled as the "shopbook rule" of "business records exception," this exception permits introduction into evidence of records and documents created in the normal course of an ongoing activity or enterprise.[29]

Admissions: This family of exceptions is the commonest vehicle for admission of e-mail, because of the nature of the evidence -- these are statements being used against the person who made them.[30]

---

[26] *See, e.g., Atlantic Container Line and Others v Commission*, T191/98 (European Union Court of Justice, Court of First Instance 2003) (e-mail as evidence in a commercial dispute); *Pflugradt v BCE*, T178/00 (European Union Court of Justice, Court of First Instance 2002) (e-mail as evidence in employment dispute);
[27] Australia Evidence Act 1995 § 59.
[28] *R. v. Schwartz*, 2 S.C.R. 443, Supreme Court of Canada (1988) para. 58.
[29] *See, e.g.,* Canada Evidence Act § 30.
[30] *See, e.g.,* Australia Evidence Act 1995 § 81 et seq.

Official or Government Records: This exception is similar to the shopbook rule, except that it applies to records created in the fulfillment of official government duties.[31]

Documents with Independent Legal Significance: Items such as contracts or deeds, which because of their inherent nature give rise to legal obligations or rights.

For each kind of exception, it must be proven in court (except in cases where the admission is unchallenged or stipulated) that the evidentiary object whose admission is being sought meets the criteria applicable to that exception. For example, in most United States jurisdictions, admission of a document as a business record requires that the proponent prove that the document was made:

- at or near the time of the event it records;
- by a person with knowledge of the event;
- as part of a regular system of records;
- in which it was the regular practice to make this kind of record.[32]

The proof is normally made by testimony from a qualified witness, and is achieved when the presiding judge is satisfied by the testimony given.

In the case of electronic records such as e-mail, additional proof may be required:

> "Any person seeking to admit an electronic document as evidence has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic document is that which it is purported to be."[33]

This may require an additional round of testimony to establish the conditions under which the record was created or stored, or to establish that the electronic record was actually created or sent by the purported sender.[34] Thus, the party seeking admission of an e-mail must typically meet two standards: first, that the document's contents meet the criteria for a hearsay exception, and second, that the e-mail itself and the system on which it was created meet the local criteria for admission of electronic records.

The rules in effect may contain provisions explicitly intended to facilitate admission of electronic records:

> "(1) Writings and recordings. "Writings" and "recordings" consist of letters, words, or numbers, or their equivalent, set down by handwriting, typewriting, printing,

---

[31] *See, e.g.,* Id. § 153 et seq.
[32] United States, *Uniform Rules of Evidence,* Rule 803(6), in force in federal courts and 46 of the 50 states.
[33] Canada Evidence Act, § 31.1.
[34] *See, e.g., People v. Bovio,* 455 N.E.2d 829 (Ill. App. 1983) (United States), requiring extensive foundation (background) testimony about the nature of a computer system as a prerequisite for admission of electronic records. Note also that most of this requirement has since been eliminated.

> photostating, photographing, magnetic impulse, mechanical or electronic recording, or other form of data compilation.
>
> * * * * *
>
> (3) Original. An "original" of a writing or recording is the writing or recording itself or any counterpart intended to have the same effect by a person executing or issuing it. An "original" of a photograph includes the negative or any print therefrom. If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original".
>
> (4) Duplicate. A "duplicate" is a counterpart produced by the same impression as the original, or from the same matrix, or by means of photography, including enlargements and miniatures, or by mechanical or electronic re-recording, or by chemical reproduction, or by other equivalent techniques which accurately reproduce the original."[35]

Such language places electronic documents on a par with their paper counterparts, and thus reduces the burden of admissibility largely to one of ensuring that the evidence meets the requirements of one of the hearsay exceptions. There is also, on occasion, language directly intended to facilitate admission of objects such as e-mail:

> The hearsay rule does not apply to a representation contained in a document recording a message that has been transmitted by electronic mail or by a fax, telegram, lettergram or telex so far as the representation is a representation as to:
>
> (a) the identity of the person from whom or on whose behalf the message was sent; or
>
> (b) the date on which or the time at which the message was sent; or
>
> (c) the message's destination or the identity of the person to whom the message was addressed.[36]

This again eliminates a portion of the proof necessary to get an e-mail into evidence. The United Kingdom has gone even further, eliminating the hearsay rule altogether in civil proceedings: "In civil proceedings evidence shall not be excluded on the ground that it is hearsay."[37]

The foregoing is necessarily a somewhat general discussion. There are a number of common law jurisdictions in the world, and they collectively employ a number of statutes, rules and case decisions in this area. Further, many of the larger common law countries are themselves divided into provinces, states or other subdivision, each with autonomous courts and legislatures, and

[35] Colorado (United States).Court Rules, Rules of Evidence, Rule 1001.
[36] Australia Evidence Act 1995 § 71.
[37] United Kingdom, Civil Evidence Act 1995 § 1.

each of these in turn has its own evidentiary rules. Resolving precise questions of admissibility in any jurisdiction will require resort to the applicable law of that jurisdiction or sub-jurisdiction. In practice, however, common law courts have admitted e-mail into evidence in a wide variety of circumstances. Canadian courts have admitted it in contract disputes,[38] as evidence in criminal cases[39] and in domestic cases[40] among other situations. Canadian courts have also concluded that recovered e-mails are potentially admissible even if the recovery is incomplete, leaving gaps in the text.[41]

Courts in other jurisdictions view e-mail similarly. Australia,[42] New Zealand,[43] the United States[44] and the United Kingdom[45] all have extensive bodies of case law in which e-mail has been successfully introduced into evidence in a variety of situations for a variety of purposes.

3.3. Administrative Proceedings and Environments

The above discussion contemplates actual litigation in a formal court setting. There are, in addition, a number of other legal and quasi-legal settings in which evidence is taken and judgment rendered. These include low-level legal tribunals such as drivers' license revocation hearings, administrative boards such as zoning and planning boards and other permitting bodies, and other decision-making entities such as government benefits administrators, tax boards and the like. Every legal jurisdiction in the developed world -- national, provincial and local -- has them, and the larger jurisdictions have hundreds of them. In jurisdictions such as Canada, the United States and Australia, each of the provinces or states has its own body of them, further complicating matters. Like courts, these bodies receive evidence and render decisions, often on important matters. Thus, their evidentiary rules and practices are important.

The number of jurisdictions and number of such entities does not permit formulation of a general rule concerning the evidentiary use of e-mail in them. They may be governed by the provisions of a general set of rules applicable to all such bodies within the jurisdiction,[46] or they may be

---

[38] *See, e.g., Champion International Corp. v. Sabina (The)*, 2002 FCT 1122 (Federal Court of Canada, Trial Division 2002).
[39] *See, e.g., R. v. Ungaro*, 2003BCPC137 (Provincial Court of British Columbia 2003).
[40] *See, e.g., K. (K.B.) v. K. (J.L.*), 2001SKQB573 (Saskatchewan Court of Queen's Bench 2001).
[41] *R. v. Evans*, 2002BCSC1674 (Supreme Court of British Columbia 2002).
[42] See, e.g., *Neat Domestic Trading Pty Limited v AWB Limited* [2003] HCA 35 (High Court of Australia 2003) (e-mail as evidence of contract negotiations and obligations); *Haynes v. Hughes* WASCA 146 (Supreme Court of Western Australia, Court of Appeal 2001) (e-mail as evidence of unlawful possession of pornography).
[43] *See, e.g., The Queen v. Lawrence Roy Hooker* NZCA 208 (New Zealand Court of Appeal 2003) (e-mail as evidence of drug dealing); Auckland *Regional Council v. John William Sanson* NZCA 313 (New Zealand Court of Appeal 1999) (e-mail as evidence of conduct in an employment dispute).
[44] *See, e.g., United States v. Microsoft*, No. 00-5212 (D.C. Cir. 2001) (e-mail as admission in anti-trust case); *United States v. Whitesell*, 02-12655 (11th Cir. 2002) (e-mail as evidence in the sentencing phase of a child pornography case); *People v. Thousand*, No. 220283 (Mich. App 2000) (e-mail as evidence in a child pornography case).
[45] *See, e.g., Coopers Payen Ltd & Anor v. Southampton Container Terminal,* EWCA Civ. 1223 (England and Wales Court of Appeal (Civil Division) 2003) (e-mail as evidence in a suit over damages from an industrial accident); *Snowstar Shipping Company Ltd. v. Graig Shipping Plc & Anor* EWHC 1367 Comm. (England and Wales Court of Appeal (Commercial Division) 2003) (e-mail as evidence in a contractual dispute).
[46] *E.g.*, The Administrative Procedure Act, a statute in place in most American jurisdictions, which contains rules by which the administrative bodies of the jurisdiction must conduct hearings, receive evidence and render decisions.

governed by a specific set of rules applicable only to the body in question. Such rules may be narrow indeed:

> "5.04 (1) If a proceeding is commenced by or against a partnership using the firm name, any other party may serve a notice requiring the partnership to disclose immediately in writing the names and addresses of all partners constituting the partnership at a time specified in the notice; if a partner's present address is unknown, the partnership shall disclose the last known address. O. Reg. 258/98, r. 5.04 (1).
>
> Use of E-Mail
>
> (1.1) The disclosure required by subrule (1) may be made by e-mail as provided by rule 8.09 if the person making the disclosure is entitled to use electronic documents in the proceeding under rule 1.06. O. Reg. 461/01, s. 4 (1)." [47]

In this example, use of e-mail is permitted for a *specific* notification to a *specific* class of party under *specific* circumstances, all applicable to that tribunal in that jurisdiction only. This is not uncommon: many of these bodies operate under their own rules of practice and procedure. This pattern of balkanization and specificity requires that the applicable rules for the tribunal or body in question be consulted prior to making a judgment about the acceptability of e-mail or similar items before that particular body or tribunal. Notwithstanding this complexity, it is possible to state as a general proposition that such bodies have more relaxed and informal rules regarding the submission of evidence before them than to the courts:

> "This kind of tribunal [professional disciplinary tribunals] is required to apply procedural fairness but is not limited by the formal processes and procedures developed by the courts or necessarily bound by the strict rules of evidence."[48]
>
> "Since administrative tribunals are in charge of evidentiary matters, they may allow any evidence, even if it is indirect. As a general rule, hearsay evidence is admissible before quasi-judicial tribunals provided they comply with the rules of natural justice."[49]

Therefore, as a general proposition, use of e-mail for evidentiary purposes before such bodies will be at least as easy, and in many or most cases easier, than in the courts of the same jurisdiction.

3.4. Conclusion -- Evidence

Although electronic records went through a long period in which their acceptance in legal proceedings was subject to attack or limitation, e-mail as a legal phenomenon appeared relatively late in that process. By that time, the acceptance of electronic records had been in large part

[47] Ontario (Canada) Regulation 258/98, Rules of the Small Claims Court, Rule 5.04.
[48] *O'Neil, Nick,* "Tribunals - They need to be different" The Australian Institute of Judicial Administration, Fourth Annual AIJA Tribunals Conference.
[49] Canada Board of Referees, *Tribunal Proceedings*, 3.3.6., para. 3, www.ei-ae.gc.ca/board/tribunal/Thome_e.shtml.

established, and a generation of users had arisen that was familiar with electronic technology and comfortable with the reliability of e-mail. E-mail is currently treated much as any other documentary evidence: it may be subject to proof requirements regarding authenticity or reliability; and must overcome any pertinent evidentiary bars such as hearsay rules. If this is done, courts appear to have little trouble accepting e-mail as evidence. Recent decisions from all jurisdictions are noteworthy in their ready acceptance of e-mail by both the court and the litigants. E-mails are treated much like any other document or admission, and little if any time is expended on questions of whether e-mail is a suitable evidentiary medium.

4. E-Mail as a Transactional Record

An e-mail-related topic of considerable importance in the context of records retention is that of EDI transactions. Web interfaces, e-mail and similar devices permit commercial transactions of many types to be conducted in whole or in part via EDI. There may be, as is the case in point-and-click transactions, formal pre-written contract language imbedded in the transaction as well as more formal documents in the form of on-screen order forms to be filled out and so on -- as well as confirmatory e-mails. On the other hand the transaction might also consist entirely of traditional e-mail documenting the various parts of the transaction -- offer, acceptance and defined terms -- required to create a legally binding relationship. In either event, the transaction poses certain difficulties from the standpoint of traditional transaction verification.

- Authentication of the party on the other end of the transaction is problematic: the parties are not face-to-face, and may even be strangers.
- Traditional proof that communications in the transaction come from the party they are alleged to have come from are similarly problematic;
- Courts might not recognize an EDI-based transaction as creating a binding relationship;
- Many EDI-related transactions are conducted in whole or in part by automated systems (such as, for example, the aforementioned point-and-click processes), creating doubts as to whether offer and acceptance in the traditional sense have occurred. This again creates uncertainty about the existence of a binding relationship.

The uncertainty raised by these issues does not serve to explicitly prohibit electronic commerce and contracting, or the use of e-mail in conducting government business. There is no general requirement that contracts be "written" or paper-based in either civil law or common law jurisdictions, nor is there any fundamental legal requirement that government business or contacts with government be conducted in a paper-based medium. The newness of the technology did, however, create uncertainty as to the legal status of any these transactions being conducted by means of it:

"Written" contracts: Although there is no general prohibition on non-written or oral contracts, there are some situations where (in some jurisdictions) a writing is required in order to create an enforceable contract. These include:

- Employment contracts -- many jurisdictions require employment contracts to be in writing;[50]
- Sales contracts over a certain monetary value;[51]
- Contracts for sale of real property.[52]

The question that arises in this situation is whether e-mail or other EDI constitutes a "writing" sufficient to meet this requirement.

Signatures: In some situations, a communication must contain a signature to be valid or binding. The concern arises here that a "signature" created or transmitted by EDI might not be binding in the manner of a manually written signature.

Timing: Any transaction in which the parties are not communicating in real time poses a legal question of timing: At what moment did each action occur? Many transactions are highly time-sensitive, and the precise timing of an acceptance of an offer, or the withdrawal of that offer, may be very critical in the event of a subsequent dispute.

These uncertainties have been resolved through application of a number of legal devices. Some have involved new laws or legal concepts. Others have been re-visitations or fresh applications of existing law and doctrine.

4.1. E-Mail as a "Writing" or "Record"

Both civil and common law traditionally viewed a "writing" as being a paper-based object. However, the technological assault on the paper-based view of the law is not a new one. The invention of the telegraph, and its immediate use in commercial affairs, presaged the legal issues surrounding e-mail. Analytically, a telegraph message is similar to e-mail -- the data is input on one end, encoded and transmitted electronically to a recipient and assembled on the receiving end into a persistent record for delivery and reading. Thus, in situations where the law contemplates the use of telegraph messages, it is a short conceptual leap to the use of e-mail.

The law has long explicitly contemplated and authorized the use of telegraph messages in commercial and other legally significant transactions, generally in a manner that equates it to a writing originating on paper:

> "Commercial contracts can be proven by: . . . Written and telegraphic correspondence . . . ."[53]

---

[50] *See, e.g.*, South Africa Basic Conditions of Employment Act § 29; Sweden Employment Protection Act § 6A, among others.

[51] *E.g.*, The Uniform Commercial Code (enacted into law in many United States jurisdictions) § 2-201 (any contract for the sale of goods valued at over $500 to be memorialized by a writing " sufficient to indicate that a contract for sale has been made between the parties and signed by the party against whom enforcement is sought or by his authorized agent or broker.")

[52] The so-called *Statute of Frauds*, originally an English statute (29 Car. II c.3) adopted in some form by most of the United States, and providing that certain classes of contract are unenforceable unless memorialized by a writing signed by the party against whom enforcement is sought or their agent.

or

> The term "prescription" as . . . means an order for drugs or medicines or combinations or mixtures thereof, written or signed by a duly licensed physician, [or other health care professional] . . . transmitted to pharmacists through word of mouth, telephone, telegraph or other means of communication . . . and such prescriptions received by word of mouth, telephone, telegraph or other means of communication shall be recorded in writing by the pharmacist and the record so made by the pharmacist shall constitute the original prescription to be filed by the pharmacist . . . .[54]

For such provisions, it is a short step to include e-mail in the same manner by mere inclusion of in the list of approved communications, or by a statutory construction which ether equates e-mail to telegraphic communication, or finds its implied inclusion in the list of "other" communications. Provisions such as this:

> "Merchants shall preserve for ten years the original of letters, telegrams, data messages or any other documents in which contracts are formalized, or which contain covenants or commitments giving rise to contractual rights and obligations."[55]

underwent this precise process -- the term "data message" was simply appended onto a much older provision, with the clear intent of including e-mail in a broad class of business correspondence including traditional letters and telegrams.

Other enactments and amendments more explicitly contemplate or authorize e-mail as an acceptable alternative to traditional paper methods. Thus, for example, a law requiring that a drivers' license revocation report be made in a "form approved by the registrar" was amended to require that it be made in a "format approved by the registrar," and delivery was authorized "in any form, including electronic or otherwise, that the registrar deems appropriate."[56] A reviewing court concluded that these revisions demonstrated a clear intent by the legislature to permit transmission of the report by e-mail and similar means.[57]

Other regulations extend the concept of e-mail as a written document to situations governing the mandatory retention of written documents, thus requiring the mandatory retention of e-mail. This is most likely to be the case where the e-mail's custodian is a fiduciary or other professional whose communications to clients have considerable financial or legal impact, or whose position gives rise to the possibility of undue influence, fraud or other violations of their duty to their client. For example, the United States Securities and Exchange Commission (SEC) by regulation requires investment advisors to retain:

---

[53] Argentina Commercial Code, § 208.
[54] New Jersey (United States) Statutes, § 45:14-14.
[55] Mexico Commercial Code Art. 49.
[56] 90 M.G.L. § 24(1)(f,(1), (Massachusetts, United States).
[57] *Doherty v. Registry of Motor Vehicles*, (No. 97CV0050 Suffolk D.C. 2001) (Massachusetts, United States).

> "Originals of all written communications received and copies of all written communications sent by such investment adviser relating to (i) any recommendation made or proposed to be made and any advice given or proposed to be given, (ii) any receipt, disbursement or delivery of funds or securities, or (iii) the placing or execution of any order to purchase or sell any security."[58]

The same agency interprets this to mean that:

> "The substantive requirements and liability provisions of the federal securities laws apply equally to electronic and paper-based media. For example, the antifraud provisions of the Exchange Act and Rule 10b-5 thereunder, as well as section 206 of the Advisers Act and the rules thereunder, apply to information delivered and communications transmitted electronically, to the same extent as they apply to information delivered in paper form."[59]

Nor is this trend limited to the United States. Australian legislation provides that, among the methods by which the pertinent minister may "give a document to a person" is "transmission by fax, e-mail or other electronic means;" to "the last fax number, e-mail address or other electronic address, as the case may be, provided to the Minister by the recipient for the purposes of receiving documents."[60] In this instance, the analogy to regular mail is complete: electronic addresses of all types are treated as functionally identical to their geographic counterparts.[61]

Case decisions take a similar tack. *Armstrong v. Executive Office of the President*,[62] an early case concerning preservation of e-mail in the context of a public records preservation statute, concluded that e-mails "made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business;" and "preserved or appropriate for preservation by that agency . . . as evidence of the agency's organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in [it]"[63] were indeed public records in the same manner as other, more traditional written documents. Other cases have concluded that e-mail is a writing in the context of a contractual dispute,[64] that e-mail is "writing" or "document" in the context of a criminal search warrant,[65] that e-mail is "correspondence" indistinguishable from other correspondence for purposes of a search warrant,[66] and that e-mail is a "writing" sufficient

---

[58] United States Securities and Exchange Commission, *Rules and Regulations, Investment Advisers Act of 1940*, 17 C.F.R. §275.304-2.

[59] United States Securities and Exchange Commission, *Interpretive Release No. 33-7288, Use Of Electronic Media by Broker-Dealers, Transfer Agents, and Investment Advisers for Delivery Of Information; Additional Examples under The Securities Act Of 1933, Securities Exchange Act Of 1934, And Investment Company Act Of 1940* (May 9, 1996), f.n. 4. *See also, Use of Electronic Media for Delivery Purposes, Release No. 33-7233; 34-36345 (October 6, 1995).*

[60] Australia Migration Act 1958, § 494B

[61] *See also* Australia Customs Act, §§ 4 & 243W, f.n. 12 and 13, supra.

[62] *Armstrong v. Executive Office of the President*, 1 F.3d 1274 (D.C. Cir. 1993) (United States).

[63] *Armstrong* at 1283.

[64] *Cloud Corp. v. Hasbro, Inc.*, No. 02-1486 (7th Cir. 2002) (United States) (concluding that an e-mail was a "writing" that satisfied the statute of frauds). *See*, 4.1. supra, and f.n. 52.) .

[65] *United States v. Wong*, No. 10070 (9th Cir. 2003) (United States).

[66] *State v. Roesing*, CR00103351 (CT. Sup Ct. 2001) (United States).

to satisfy the statute of frauds in a real estate transaction;[67] and as observed in 3.1. above, e-mail as been accepted in evidence without analysis in many other cases.[68]

The bodies of both statutory and case law are by no means comprehensive on this issue -- there are many situations where the issue has not been explicitly addressed, or where the language of a particular statute or regulation might lead to a contrary result. Nonetheless, it appears as though a consensus has emerged: Absent a clear legislative intent otherwise, E-mail is a 'written" object, and so subject to the same rules and doctrines as more traditional written documents.

4.2. E-Mail as a Government or Public Record

Many of the statutes, regulations and court cases cited above involve public records, and the question of whether e-mail or EDI is a suitable medium for recording such a transaction. This is not surprising: government records, required submissions to government and "written" contacts with government are subject to various archives and records laws, and in addition to their use in regulatory schemes and enforcement, are often subject to public scrutiny be means of open records laws. Complicating the resolution to the public records issue are two factors: the number of individual agencies or bodies which may potentially use or receive e-mail; and the fact that these bodies may have individualized rules and restrictions on communications methods that may be used with them. It can be stated as a general rule, however, that e-mail, whether internal e-mail from and to government employees, or e-mail received from outside parties, is a government record, provided that it records government activities or business. In the United States federal arena, this was definitively established by *Armstrong v. Executive Office of the President*, and subsequent implementing regulations.[69] State governments take a similar position:

> "E-mail messages are potentially official government records, so you should plan for e-mail as part of your electronic records management strategy. The medium is irrelevant. The content of the message determines whether it is a record or not; the content determines to which records series the message belongs; and the content determines how long the message needs to be retained."[70]

Australia's National Archives takes a similar position:

> "All digital data created or received in the conduct of Commonwealth business are Commonwealth records under the Archives Act 1983 and need to be managed in accordance with the Act. Commonwealth Government agencies must manage electronic records with the same care as they manage paper records."[71]

---

[67] *Shattuck v. Klotzbach*, 2001 Mass. Super. LEXIS 642, No. 011109A, 2001 WL 1839720 (Mass. Super. 2001) (United States).
[68] *See*, Se. 3.1 supra, and f.n. 42-46.
[69] *See*, f.n. 60, supra. *See also* NARA implementing regulations at 36 C.F.R. Part 1234.
[70] Minnesota (United States) State Archive, *Electronic Records Management Guidelines*, http://www.mnhs.org/preserve/records/ electronicrecords/eremail.html.
[71] *See* Website of the National Archive of Australia/Recordkeeping/Electronic Records, http://www.naa.gov.au/ recordkeeping/er/summary.html. *See also* Australian Guidelines on Managing Electronic Records as Documents.

As have New Zealand:[72]

> "The phrase '*any kind whatsoever*' makes it clear that it is the intention of the Act to cover all public records regardless of format."[73]

Canada:

> "An e-mail message, including any electronically attached documents, containing information created, collected, received or transmitted in the normal course of government business, sent via an e-mail system, is a record."[74]

and the United Kingdom.[75]

There seems little doubt at this point that e-mail sent or received by government is considered as a public record, subject to whatever formal management requirements are in place within the jurisdiction. There appear to have been few or no serious court challenges to this doctrine in recent years.

4.3. E-Mail as a Tool for Transmitting Information to Government

More problematic is the question whether e-mail is an adequate communication medium for required filings or required information collection, or for transacting other "official" business with government. The concept of "e-government" has gained a certain cachet in recent years, due to its supposed efficiencies, and as a result, many government agencies now collect information of various kinds through EDI transactions definitionally and analytically indistinguishable from e-mail. Noteworthy examples in the United States include the Securities and Exchange Commission (SEC), which permits submission of financial reports on publicly traded companies via its Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system,[76] as well as required data for an assortment of other regulated parties; the Internal Revenue Service (IRS) for a wide variety of tax-related forms and data.[77] An assortment of other state and federal agencies have similar systems.[78] Similar systems are in use elsewhere: Canada's Corporations

---

[72] *See* Archive New Zealand ,*Electronic Records Policy*, http://www.archives.govt.nz/statutory_regulatory/er_policy

[73] Id. at FAQ's, responding to the question whether electronic records are covered by the Archives Act, notwithstanding that electronic records are nowhere mentioned in it.

[74] National Archive of Canada, E-*Mail Management in the Government of Canada* p. 2, http://www.archives.ca/06/060404_e.html.

[75] S*ee generally*, United Kingdom Public Records Office, *e-Government Policy Framework for Electronic Records Management*, http://www.pro.gov.uk/recordsmanagement/erecords/default.htm.

[76] *See* 17 C.F.R. Part 232 EDGAR filing system Regulation S-T General Rules and Regulations for Electronic Filings Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system.

[77] *See, e.g.*,http://www.irs.gov/efile/index.html

[78] *See, e.g.*, Pennsylvania e-TIDES (Electronic Tax Information and Data Exchange System), http://www.etides.state.pa.us (tax filing); California Secretary of State, http://www.ss.ca.gov/prd/electronic_filing_info.htm (inter alia, lobbying reports, political contributions); Idaho State Tax Commission, http://www2.state.id.us/tax/filing.htm (tax filing); Georgia Environmental Protection Agency, http://www.ehso.com/stategaenvforms.php (hazardous waste filings), among many others.

Agency permits electronic filing of corporation documents,[79] as does the Canada Customs and Revenue Agency,[80] among others. Australia,[81] New Zealand,[82] Hong Kong[83] and other jurisdictions have similar schemes in place. These schemes amount to dedicated e-mail systems for transmission of required information. In addition to these dedicated systems, governmental agencies also have extensive listings of e-mail addresses for purposes of general correspondence, advice, complaint submittal and other activities.[84] Any of these vehicles is capable of transmitting information between a government entity and another party that is either legally required, or is part of an authorized transaction between government and the other entity that may result in consequences for the other party.

Although it may be stated as a general rule that government agencies are open to these kinds of communication schemes, it is important to note that each example cited above, and most of the many other examples that can be found, is an individualized case -- there is no general rule of law requiring that an agency offer or accept e-mail as a communication medium for official business,[85] and no universal practice of doing so. Many such schemes are governed entirely by rules of practice generated within the controlling agency or entity. In cases where the communication in question is important, the rules and practices of the entity in question control. In cases where it is authorized, however, the e-mail or its attachments may be evidentiary objects or regulatory compliance objects of considerable importance, and the transmittal data proof of compliance with deadlines or other requirements.

4.4. E-Mail in Commercial Transactions

The pervasive use of EDI in commercial settings required that the uncertainty about the validity of commercial transactions conducted through it be eliminated. This brought about the passage of laws governing the legality of EDI, and which are germane to the legality of e-mail. Perhaps the most important of these is the United Nations Commission on International Trade (UNICTRAL) Model Law on Electronic Commerce. In one form or another, this law has been enacted into force in at least 31 countries.[86] Other countries[87] have adopted digital signature

[79] *See*, Corporations Canada Electronic Filing Centre, http://strategis.ic.gc.ca/sc_mrksv/corpdir/corpFiling/engdoc/index.html

[80] *See*, http://www.ccra-adrc.gc.ca/eservices/tax/business/efile/menu-e.html.

[81] See, e.g., Federal Court f Australia, https://www.efiling.fedcourt.gov.au/fedcourt/WelcomeToFedCourtEFS.htm (court filings); IP Australia, http://www.ipaustralia.gov.au/about/site_privacy.shtml (intellectual property filings), among others.

[82] *See, e.g.*, New Zealand Inland Revenue E-File System, http://www.taxweb.co.nz/efile.htm (tax filing).

[83] *See, e.g.*, Hong Kong Electronic Financial Filing System, http://man.aect.cuhk.edu.hk:10080/help/about.phtml (required financial filing).

[84] E.g., United States SEC, http://www.sec.gov/contact/mailboxes.htm; United States Environmental Protection Agency, http://www.epa.gov/epahome/hotline.htm; Australia Workplace, http://www.workplace.gov.au/Workplace/WPFeedback/0,1337,a0%253D0%2526a1%253D517%2526a2%253D517,00.html; among many others.

[85] In the United States, for example, required submissions to government agencies are among the handful of enumerated exceptions to the broad authorization of electronic transactions in the so-called E-Sign Act. *See, Electronic Signatures in Global and National Commerce Act*, § 104 (a).

[86] Bermuda (*Electronic Transactions Act of 1999*); Canada (*Uniform Electronic Commerce Act*); Ecuador (*Law Governing Electronic Commerce, Electronic Signatures, and Data Messages*); European Union (Austria, Belgium,

legislation, generally modeled on the UNICTRAL Model Law on Electronic Signatures, which also impacts e-mail.

UNICTRAL and its progeny and variants have many provisions germane to an e-mail analysis:

> "Data message" means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy."[88]
>
> "Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message."[89]
>
> "Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message."[90]
>
> Where the law requires information to be in writing, that requirement is met by a data message if the information contained therein is accessible so as to be usable for subsequent reference.[91]
>
> "[The preceding] Paragraph applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing."[92]
>
> "Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if: (a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and (b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented. "[93]

Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, Netherlands, Portugal, Spain, Sweden, United Kingdom) (via *Directive 2000/31/EC Of The European Parliament and of The Council*); Guernsey (*Electronic Transactions (Guernsey) Law 2000*); Hong Kong (*Electronic Transactions Ordinance*); India (*Information Technology Act 2000*); Jordan (*Jordan Electronic Transactions Law No. 85 of 2001*); Mauritius (*The Electronic Transactions Act 2000*); New Zealand (*Electronic Transactions Bill*); Philippines (*Electronic Commerce Act of 2000 - Republic Act 8792*); Republic of Slovenia (*The Electronic Commerce and Electronic Signature Act*); Singapore (*Electronic Transactions Act of 1998*); Republic of (South) Korea (*The Basic Law on Electronic Commerce*); Tunisia (*Electronic Exchanges and Electronic Commerce Law*); Turks and Caicos Islands (*Electronic Transactions Ordinance 2000*); United States (*Electronic Signatures in Global and National Commerce Act*; *also see* the *Uniform Electronic Transactions Act (UETA)*, which contains many provisions with nearly identical language).

[87] Argentina, Brazil; People's Republic of China; Czech Republic; Estonia; Gibraltar; Hungary; Israel; Japan; Lithuania; Malaysia, Mexico; Peru; Poland; Romania; Russia; Thailand.

[88] UNICTRAL Model Law on Electronic Commerce, Art. 2 (a).

[89] *Id.*, Art. 5.

[90] *Id.*, Art. 5 bis.

[91] *Id.*, Art. 6 (1).

[92] *Id.*, Art. 6 (2).

[93] *Id.*, Art. 8 (1).

"[The preceding] Paragraph applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing."[94]

"In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence: (a) on the sole ground that it is a data message; or, (b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form."[95]

"Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor."[96]

"Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied: (a) the information contained therein is accessible so as to be usable for subsequent reference; and (b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and (c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received."[97]

"In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose."[98]

There are, in addition to these provisions, rules governing other issues, including timing of offers and acceptances[99] ratification of automatically generated e-mail[100] and signatures.[101] These provisions place e-mail (and other EDI transactions) squarely on a par with traditional paper-based or in-person transactions. In jurisdictions having adopted the model signatures law, a similar, if less comprehensive result obtains: data messages and the electronic signatures thereon are validated if certain standards are met.[102] Thus, in any UNICTRAL jurisdiction, e-mail may constitute a very important document trail for either regulatory compliance or commercial purposes. And as we have seen, e-mail has readily been admitted into court in many jurisdictions for just such purposes. It is reasonable to expect that over time, the model law will

[94] *Id.*, Art. 8 (2).
[95] *Id.*, Art. 9 (1).
[96] *Id.*, Art. 9 (2).
[97] *Id.*, Art. 10 (1).
[98] *Id.*, Art. 11.
[99] *Id.*, Art. 15.
[100] *Id.*, Art. 13.
[101] *Id.*, Art. 7.
[102] UNICTRAL Model Law on Electronic Signatures (2001) Art. 6.

be adopted in other jurisdictions, and that courts in additional jurisdictions will reach similar conclusions.[103] A final case on e-mail illustrates the legal system's progressive willingness to entrust significant transactions to e-mail:

In the United States, service of legal process[104] prior to commencement of a lawsuit is normally a process involving a considerable number of paper-based formalities. The documents served on the defendant are normally paper; the service is in-person (even such means as registered mail are not normally permitted); and paper attestations to the delivery of the documents are then made. In a recent case, normal service of process could not be had on a defendant due to their off-shore location and efforts to avoid being served. Upon application by the plaintiff and a showing of extraordinary circumstances, service of process by e-mail was permitted by the trial court, and the procedure was upheld on appeal.[105]

This is an extraordinary case, and highly unusual facts. It is nonetheless illustrative of the extent to which the legal system is beginning to trust e-mail for the delivery of highly significant documents.

4.5. Conclusion -- E-Mail as a Transactional Record

For purposes other than required submissions of information to government, there is little doubt at this point that e-mail is a viable evidentiary and audit trail. In some cases, retention of e-mail is required by law, either as a record of a business transaction, or as a public record. In other cases, retention of e-mail is not required by law; the law merely validates its use. Nonetheless, if transactions are conducted in those cases in whole or in part by e-mail, its retention may be a vital component in proving compliance or resolving disputes. There is little doubt that properly maintained e-mail will have evidentiary value before any tribunal in the event such a need arises.

With respect to government submissions, the picture is more complex -- many agencies in many jurisdictions authorize or permit e-mail contact; but whether that e-mail contact is legally valid or binding is an issue that must be decided on a case-by-case basis. There nonetheless are many instances where it may be used, and there is a trend toward an increased usage of it for this purpose.

[103] *See, e.g., Židrūnas Šapalas v. AB Lietuvos Taupomasis Banka*, Supreme Court of Lithuania (2002) (PIN code for usage of payment card is an electronic signature, the equivalent of hand-made signature under Lithuanian contract law).
[104] The delivery of complaints, summonses and other legal paperwork delivered to the defendant to commence a lawsuit.
[105] *Rio Properties, Inc. v. Rio International Interlink*, 284 F.3d 1007 (9th Cir. 2002).

5.0. Counterpoint -- The Case for Short-Period E-Mail Retention

The mix of authorities above appears to lead to the conclusion that long-term categorical retention of most or all e-mail is unavoidable for many organizations. There are, however, countervailing considerations with considerable legal, business and risk management implications.

The Smoking Gun. The first and most obvious of these is the so-call "smoking gun" phenomenon. This is well-known to most corporate information managers, and consists of e-mail with embarrassing or legally damaging content. The material is commonly produced in lawsuits -- very much against the wishes of its custodian -- and has been a prominent factor in many lawsuits, some very high profile.[106]

Privacy. The second of these are privacy laws and their e-mail-related ramifications. A number of jurisdictions have adopted data privacy laws imposing very strict controls on the use and transmission of "personal" information concerning individuals, including employees of businesses. The gist of such laws is that, absent permission from the person it concerns, personal information may only be used for the lawful purpose for which it was collected, it must be maintained only for the period of time for which it is actually needed for that purpose, and it may not be transmitted to a jurisdiction which does not have a comparable level of protection in place.

Such laws are rapidly becoming very widespread,[107] and regulators are taking a broad view of what constitutes "personal: information; and even in jurisdictions without an overall privacy law, there are also a great many subject-specific laws concerning medical information, financial information, and other data.[108] E-mail's ubiquitous use as a corporate communications tool, potentially and actually used for routine transmission of personal information about employees, business partners and others thus places organizations with multinational operations at serious risk of embarrassment and of violating such laws.[109]

Cost. The third consideration is more mundane: retention of millions of e-mails for anything other than a short period of time may be very expensive, particularly if any effort is expended on categorization or indexing. Adding to this the cost of searches related to lawsuits or other legal

---

[106] *See, e.g., United States v. Microsoft*, Nos. 98-1232 (TPJ) and No. 98-1233 (TPJ) D. C. Dist. Ct. (2000) (E-mail concerning anti-competitive practices in an antitrust lawsuit); Securities and Exchange Commission v. Martha Stewart and Peter Bacanovic, 03 CV 4070 (NRB) (N.D. N.Y. 2003) (electronic messages alleged to be probative of improper stock trading); *United States v. Quattrone*, (e-mail alleged to be probative of illegal activity including spoliation of evidence)..

[107] The European Union Data Privacy Directive, the model for most such laws, is in force in the E.U., thereby affecting most of western Europe; in addition, such widespread jurisdictions as Hong Kong, Australia, India and many Latin American countries have or will shortly enact similar legislation.

[108] *See, e.g.,* regulations under the *Health Insurance Portability and Accountability Act of 1996 (HIPPA),* found at 45 C.F.R. Part 164 (United States).

[109] *See, e.g.,* The Wall Street Journal, *Online Laundry: Government Posts Enron's E-Mail*¸ October 6, 2003 p.1. (Corporate e-mail gathered by government agency as part of regulatory probe and posted on public web site found to contain personal information including social security numbers).

action in a poorly structured or completely unstructured environment could make the long-term retention of e-mail prohibitively expensive.

Proponents of short-period retention seek to mitigate the above issues by a simple device: Place a single, non-categorical and relatively short retention period on all e-mail and purge all e-mail upon expiration of that period. The benefits of this approach are obvious and substantial: Legal risks are substantially reduced simply by reducing to some minimum the backward-looking window into which an investigation or other inquiry can inquire. Smoking guns, or evidence of a violation of some privacy requirement, is either absent entirely or limited in its scope or volume. Many violations, such as retaining personal information for an excessive period of time, are avoided entirely. Costs are contained by keeping to a minimum the hardware, software and other infrastructure needed to support e-mail, and by reducing the amount of time and other resources expended on searches and other activity related to the e-mail. This approach also has the qualities of simplicity and relative ease of administration, which are highly desirable in view of the formidable cost, and administrative and technical issues inherent in any attempt to manage large volumes of e-mail on a categorical basis.

There are, of course, risks associated with such a strategy. For some parties, it may be illegal. For others, even if legal, its benefits must be weighed against the potential drawbacks of not having a large body of written communication available: Potentially useful information may be purged prior to expiration of its useful life; e-mail used to establish regulatory compliance or for some other mandatory purpose may not be available to demonstrate compliance in the event of a dispute; contracts, or modifications to contracts, may become improvable if e-mail constituted a significant part of the process. There is, in addition, the ever-present possibility that employees who feel the retention period chosen is too short will attempt to defeat the system by hiding e-mail in locations protected from purge processes. Proponents of short-term retention argue that the benefits of short-term retention so significantly outweigh the drawbacks that any penalties or other costs associated with it are justified by the benefits and should simply be accepted as part of the strategy.

An alternative which seeks to avoid these drawbacks is selective retention. In this scenario, e-mail defaults to a single, short retention period, but legally or operationally significant categories are identified, defined and segregated for longer-term retention. This strategy seeks the best of both worlds: Short-term retention of most e-mail, thereby accruing cost savings and risk reduction, while maintaining those items that appear to have operational or legal value, thereby reducing or eliminating the risks associated with blanket short-term retention.

This approach also has drawbacks, however: While identification of substantive e-mail might be conceptually simple, consistent application of any rules in a high-volume workplace environment is likely to pose a formidable challenge, and if not properly done, could lead to very inconsistent retention and the loss of a great deal of valuable or required information.

6.0 Electronic versus Paper Retention of E-Mail

Legal authorities clearly authorize the use of e-mail in many situations, and in many cases mandate its retention, either as a legal requirement, or as a matter of prudent self-interest. Assuming that the decision has been made to retain e-mail for some period of time, the question then arises, in what form ought the e-mail to be kept? There are two competing views on this matter:

- The electronic version is the more "authentic" version, or the more acceptable version for evidentiary purposes, since it is the "original," or it is more complete.

- A paper printout is as valid as the electronic version for compliance or evidentiary purposes.

Advocacy for printout-based retention is commonly premised upon the formidable difficulties inherent in attempting to retain large volumes of unstructured material such as e-mail in something analogous to a paper-based filing system, particularly in the cases of organizations without large resources available for electronic data management. Electronic retention is commonly advocated based upon a concern that valuable metadata will be lost by paper retention, thereby reducing the evidentiary, research or compliance value of the e-mail.

Legal authorities are frequently neutral on the question of electronic versus paper retention, but if anything, can be said to be somewhat paper-centric, particularly in civil law jurisdictions, where bound and stamped paper business records were for a long time required. Even in common law countries, it was until fairly recently a common requirement to create and retain records in paper format. In cases where electronic systems created the records, there were many instances where regulated parties were required to retain electronic records as printouts, rather than in electronic format,[110] and this may still be the case on occasion. Notwithstanding the many laws authorizing the use of electronic records, a few instances of paper requirements can still be found; and many laws which do authorize electronic recordkeeping do so as alternative to an explicit or unspoken default paper system.[111]

Electronic commerce or evidence laws generally authorize or ratify electronic records, but do not require them, and there is typically no indication whatever that paper is a less acceptable medium. The UNICTRAL Model Law on Electronic Commerce requires only that data messages be "usable for subsequent reference."[112] No position is taken as to what medium is most desirable for that subsequent reference. Other laws requiring maintenance of e-mail are generally silent as to final storage medium; in many cases, however, the inclusion of e-mail in a category with correspondence and telegraph messages -- both paper-based -- is indicative of a likelihood of acceptance of printout-based storage.

[110] *See, e.g.,* the pre-2002 version of the Greece Books and Records Code.
[111] *See, e.g.,* Singapore Customs Act § 90A ("For the purposes of this Act, an electronic notice or a copy thereof shall not be inadmissible in evidence merely on the basis that it was transmitted without the making or delivery of any equivalent document or counterpart in paper form.").
[112] UNICTRAL Model Law on Electronic Commerce, Art. 6 (1).

With respect to evidentiary matters, the United States Uniform Rules of Evidence provide that:

> "If data are stored in a computer or similar device, any printout or other output readable by sight, shown to reflect the data accurately, is an "original."[113]

This provision does not require the use of paper printouts, but clearly places them on a par with the original electronic data. Canada's Evidence Act provides that:

> "[A]n electronic document in the form of a printout satisfies the best evidence rule if the printout has been manifestly or consistently acted on, relied on or used as a record of the information recorded or stored in the printout."[114]

Australia's evidence act provides that the contents of a document may be proved by tendering a document that:

> "[I]s or purports to be a copy of the document in question; and . . . has been produced, or purports to have been produced, by a device that reproduces the contents ofdocuments."[115]

The United Kingdom Civil Evidence Act provides that:

> "Where a statement contained in a document is admissible as evidence in civil proceedings, it may be proved by the production of that document, or whether or not that document is still in existence, by production of a copy of that document or the material part of it, authenticated in such manner as the court may approve."[116]

In this case, the court has discretionary power to receive a printout into evidence. As a practical matter, U.K. courts, as well as courts in the other cited common law jurisdictions, routinely admit what are undoubtedly printouts of e-mails into evidence with little or no discussion of media.[117]

In the public records arena, retention of e-mail by means of printout has been widely ratified in the common law countries. In the United States, the issue was dispositively dealt with in *Public Citizen v. Carlin*[118] in 1999. In that case, a group of plaintiffs challenged federal government regulations[119] implementing a policy of e-mail retention by means of paper printout, claiming that paper retention would obliterate valuable metadata, thereby diminishing the value of the public records at is sue. The appellate court reversed a trial court and rejected these claims, noting that the value of electronic retention must be balanced against the feasibility of doing so, the funds and resources available for records management, and the operating needs of the custodian agencies.

---

[113] Uniform Rules of Evidence, Rule 1001 (3).
[114] Canada Evidence Act, § 31.2 (2).
[115] Australia Evidence Act 1995, § 48 (1) (b).
[116] United Kingdom Civil Evidence Act, § 8 (1).
[117] *See*, 3.2., supra, and f.n. 38-44.
[118] *Public Citizen v. Carlin*, 184 F.3d 900 (DC Cir., 1999).
[119] *See*, 36 C.F.R. Part 1234.

In similar manner, the Australian Archives have issued a general and media-neutral authorization for the retention of public records in reproduction format and disposition of the originals, provided that other criteria for management of public records are met,[120] based upon similar considerations of resource allocation and operating needs.

Archives New Zealand also makes electronic versus paper-based e-mail management optional with the custodian agency:

> "Archives New Zealand does not require government agencies to print and file electronic records into a paper-based filing system. How an agency manages its electronic records is an internal decision that needs to be based on an overall records management strategy. In an ideal world, records that are born digital would continue to be managed and accessed digitally. However, if records management software or internal policies do not support electronic records management, an agency may decide that the best policy is to print and file electronic records."[121]

As does the United Kingdom Public Records Office:

> "E-mail messages should be filed as records in the same way as other electronic records with a common use of procedures and decision rules in identifying formal records; whether these are filed in an electronic system, printed to paper, or dealt with in some other way according to established procedures."[122]

The foregoing authorities, while not encompassing all jurisdictions and all situations, operate in the context of a dearth of authority to the contrary. In view of the fact that courts in these jurisdictions are prepared to accept printouts into evidence, and that the governments themselves view printout-based e-mail retention as a legitimate means of carrying out their mandated records management duties, it appears that, unless a specific legal requirement with a clear contrary indication applies, paper-based retention of e-mail is an acceptable course of action.

7.0. Retention of E-Mail

As the entire foregoing discussion reveals,[123] e-mail has a very complex relationship with the legal system; it has the potential to become a legally significant object in a wide variety of circumstances. In some of these circumstances, retention of the e-mail is mandatory, subject to a regulatory scheme or other legal requirement. In other cases, retention is not required; however,

---

[120] See generally, National Archives of Australia, *General Disposal Authority for Source Records that have been Copied, Converted or Migrated* (2003).

[121] Archive New Zealand, http://www.archives.govt.nz/continuum/faq.html.

[122] United Kingdom Public Records Office, *Guidelines for Management, Appraisal and Preservation of Electronic Records*, § 3.48.

[123] And note here that the legal authorities cited in this paper are not intended to be and are not, a comprehensive citation of authority. In every category, there are a great many laws, cases or other authorities that have not been cited.

in such cases, its disposition must be carefully weighed against the potential consequences of not having the e-mail when it is needed. Any policy decisions must also account for additional complicating factors such as any potential advantages of paper-based retention, and the risk management considerations that arise from "smoking gun" possibilities or privacy laws. The mix and severity of issues in any particular case contributes to the feasibility or legality of any solution.

7.1. Mandatory Retention of E-Mail

Many organizations, either because of the nature of their activities or because of the jurisdictions within which they do business, will find themselves in the situation of being required to retain at least some of their e-mail for a legally mandated period of time: Many if not most civil law countries have a provision contained in their civil or commercial code requiring retention of business correspondence for a period of years. Some explicitly include e-mail in this category; analysis of current statutory and case law from civil law jurisdictions leads to the conclusion that other civil law jurisdictions will view e-mail similarly. Therefore, any business in a civil law jurisdiction will probably have to retain substantive e-mail business correspondence for a legally mandated period, probably a fairly long one.[124] In similar manner, e-mail generated or received by government entities in major common law jurisdictions is categorically a public record, and thereby governed by the records retention scheme of the governing public archives or records agency. Finally, some parties such as investment advisors in the United States are subject to blanket legal retention requirements on e-mail communications because of the nature of their business.

Other settings may or may not give rise to e-mail subject to mandatory retention. The vast number of regulatory agencies and schemes, each with its own particular rules of practice and procedure, and its own idiosyncrasies, defies the formulation of a general rule. The trend, however, is clear: Such agencies are tending rapidly toward use of e-mail and e-mail-like schemes for information collection and dissemination. Parties availing themselves of any these electronic schemes may well end up with e-mail or e-mail-like data objects that are subject to mandatory retention requirements.

For any business contemplating the development of an e-mail policy, identification of any mandatory retention requirements associated with e-mail appears to be a necessary first step. Regardless of its other merits, a blanket short-term retention period without provision for accommodating for any legally required exceptions is a risky proposition. For entities in heavily regulated businesses, failure to retain e-mail concerning core or regulated activities could be very costly in terms of regulatory and legal sanctions,[125] and if severe enough could jeopardize the entity's right to conduct business.

[124] Retention periods of five and ten years are commonly seen for this requirement.
[125] *See, e.g.,* CIO Update, cioupdate.com, *S.E.C. Slaps Wall Street Over E-Mail* (Dec. 3, 2002) (Five prominent brokerage houses in the United States fined $8.25 million for failing to maintain e-mail communications from brokers to other parties concerning stock analysis).

7.2. Non-Mandatory Retention of E-Mail.

Even in cases or jurisdictions where e-mail retention is not required by law, its retention may well be governed by significant legal considerations. There is absolutely no doubt that, in many jurisdictions, including most of the major jurisdictions of Europe, North America, and the Asia-Pacific area, e-mail is a viable medium for contracting and other commercial transactions, as well as other transactions resulting in legally enforceable obligations. This viability includes the introduction of e-mail into court in those jurisdictions to prove and enforce those obligations. It is equally clear that e-mail can be introduced as evidence adverse to its creator or custodian in both criminal and civil proceedings. None of these factors absolutely mandates the retention of e-mail for any particular period of time; however, if significant discussions or transactions of any kind are occurring via e-mail and if there is any significant chance that those transactions will be subject to a legal dispute, or require resort to the legal system to prove, the custodian purges them at his peril. In such cases, e-mail is analytically identical to any other documentary evidence necessary or desirable to prevail in the dispute, and is therefore subject to the same considerations concerning retention, and ideally, the same retention period.

Consideration of the desirability of long-term retention of e-mail in cases where it is non-mandatory but advisable for business or legal reasons is, therefore also a necessary step in devising a retention policy. Retention of e-mail in this scenario in itself is a complex question, involving consideration and analysis of a number of issues, including business need, various risk scenarios such as lawsuits and regulatory actions, and legal considerations such as statutes of limitation or other laws affecting risk management. In addition, non-mandatory e-mail retention must be weighed in light of privacy laws and similar considerations.

7.3. Single-Period versus Functional Electronic Retention

In view of these considerations, a blanket, single period retain-and-purge policy without alternative provisions for segregating and saving significant e-mail via some other tool such as printout storage faces some significant hurdles. Prior to selection of any single period, several factors must be considered. First, the question of legally required or significant records arises:

- Is the e-mail system used for any purpose that may generate records with a mandatory retention period?

- Is the system being used for any purpose that may generate legally significant records such as contract negotiations or contract documentation?

If either of these possibilities is in fact the case, any single retention period that is selected must:

- Be long enough to cover any legally required retention periods applicable to e-mail in that jurisdiction; and

- Be long enough to cover at least the most significant or high-risk portion of the period during which the e-mail may be needed to prove contracts or other transactions, and to

enforce any legal rights which the owner may have acquired in whole or in part via e-mail.

This may require extensive analysis of legal records retention requirements, statutes of limitation and other authority to ensure that the selected period is legally sufficient.

Assuming that the period chosen is legally acceptable, it must then also pass muster with respect to operational requirements. If the organization relies heavily on e-mail, an excessively short retention period may impair operations regardless of any legal considerations, and there may be cases where operational considerations require longer retention than do pure legal requirements. Careful analysis of operational needs is therefore required. Even if the organization generates no legally required or legally significant records via its e-mail system, operational efficiency must be considered in developing a single retention period -- significant impairment of business operations from an excessively short period may serve to completely neutralize any gains or cost savings accruing from the short period.

All of these considerations may collectively serve to lengthen the retention period far beyond that anticipated when initially contemplating single period retention. Periods as short as 30 to 60 days are often touted, and these are likely to be deficient on at least two counts:

- Legal retention periods applicable to e-mail quite commonly run to as much as five to ten years, and in some cases could be longer;

- 30 to 60 days is unlikely to meet operational requirements in cases where significant business is being conducted via e-mail -- periods of at least a year or two are likely to be the minimums revealed by operations analysis.

In cases where e-mail is being heavily used in important business operations by a tightly regulated organization, or an organization in a high-risk industry, all of the above factors when combined may well serve to make the e-mail retention period equivalent to the longest period on the organization's retention schedule. This result probably differs considerably from the outcome initially anticipated when considering a single period schedule, and negates many of the supposed advantages of single-period retention.

In summary, single period electronic e-mail retention with no alternative arrangement for storage of exceptions appears to be a viable option only if:

- E-mail is not used for the conduct of significant business or regulatory transactions; and

- The jurisdiction does not have a legal requirement for retention of business correspondence; and

- The savings accruing from disposition of the e-mail after short-period retention justify any legal risks accruing from the disposition, such as inability to enforce rights or prove contracts.

or:

- The organization is prepared to accept a single period of several years, with all of its attendant costs and other issues.

7.4. Functional Electronic Retention

In view of the potentially long periods involved, and the reality that a high percentage of all e-mail is essentially valueless within hours or days, and therefore unneeded for any legal reason, a single-period paradigm appears to impose significant unnecessary storage and search costs on any organization generating or receiving significant amounts of e-mail. The obvious answer to this dilemma is to devise functional classifications for e-mail, similar to or identical to those of paper or other electronic records, and maintain and purge e-mail based upon this classification scheme: Cost avoidance accrues because a high percentage of e-mail is purged in short order, while legally or operationally significant items are retained. Searches to recover desired objects are easier because all retained e-mail is categorized when received or shortly thereafter.

Reality is not so simple, however.

- Based upon the state of technology at the time of this writing, software-based solutions which attempt to automatically categorize e-mail are not accurate enough to rely upon;

- Categorization of millions of e-mails manually, even if done in some highly efficient manner, requires a significant commitment of resources in the form of staff time;

- Distributed categorization by end-users (as compared with centralized categorization by dedicated staff) may be done on an inconsistent basis, or be of poor quality;

- Categorization by central staff will probably be impossible in a large organization, given the volume of e-mail involved.

These factors may well combine to make functional electronic retention both more expensive and less efficient than is optimal. A variety of devices might be employed to optimize the system and make metadata capture more efficient and cost-effective: Standard headings and other identifiers, optimized popup windows with pre-selected categories, and so on. Many such devices are available today as part of software tools. Such devices impose their own costs and issues, however:

- Any rule requiring users to format e-mail in some standard pattern requires training and education -- themselves costly activities -- and will produce results only as good as the data input done by those users;

- By its nature, e-mail is not amenable to strict rules of categorization -- an e-mail may well be about more than one topic, in much the same manner as a phone call; and many e-mails are so informally written that only the parties to the conversation will have any clue at all as to what it concerns;

- Imposition of composition or usage rules to avoid these issues will significantly impair the utility of e-mail as a communication tool, and will impose a cost in the form of the staff time spent composing formally constructed e-mail;

- Any limitations in the software will limit the accuracy of results, and the software itself is only useful if personnel actually use it. If the software is at all difficult to use, this may itself be a significant barrier;

- Any retention rules imposed on e-mail must correspond with those for similar functional objects in other media and formats; this will require e-mail software capable of enforcing retention rules, or some sort of interface between the e-mail management program and whatever tool is being used to manage retention for other data objects.

Thus, as with non-categorical retention, functional retention of e-mail is a strategy whose benefits must be weighed against the costs, often hidden, of doing so.

7.5. The Role of Paper-Based Retention

Another alternative is paper-based (printout) retention, or its electronic analogue, maintenance of e-mail as word-processing files. This option has significant advantages:

- There is no need to create an indexing of filing or indexing systems for e-mail -- it is simply incorporated into whatever filing system is already in place, including its retention periods;

- Sophisticated e-mail management software is unneeded; if any records management software is in use, it can be used to manage e-mail in the same manner as other data objects;

- E-mails related to other data objects such as contracts can be physically filed with them (or stored in the same computer directories and folders), making file review and similar activities easier and more complete;

- Little or no specialized training is needed -- most e-mail users will be able to print e-mail, or copy to a text file, with little or no additional training.

There are, however, issues:

- A large e-mail systems mean a large numbers of printouts, with the burdens attendant upon an increased paper load -- more file cabinets, box storage, etc. -- for the organization;

- Staff may be inconsistent about printing out e-mail, leading to poor results and inconsistent retention;

- Issues of informality and multiple topics are still present, with their attendant filing conundrums;

- Full-text searches and similar electronic options are not available with printouts.

These issues must be weighed against the conceptual simplicity of the approach. As with every other option, a cost/benefit analysis must be performed prior to implementation to ensure that this is a viable and cost-effective course of action.

7.6. Weighing the Options

There appears to be no ideal solution to e-mail retention -- each option imposes significant costs and burdens upon the implementing organization. Which of these costs and burdens are most palatable depends upon a number of factors:

- The size of the organization;

- The nature of the organization's activities;

- The criticality of e-mail retention and of accurate and complete retrieval;

- The volume of e-mail involved;

- The specifics and adaptability of e-mail systems and other technology already in place;

- The funds available for purchase and implementation of technology-based solutions, and the willingness to purchase and implement costly and complex solutions;

- The sophistication of users, and their willingness and ability to comply with any rules imposed as part of the solution.

7.6.1. Retention Periods

For some organizations – small organizations of all kinds, organizations which do not rely heavily on e-mail, or organizations with simple business processes or which generate and receive relatively small volumes of e-mail -- single-period retention, even if that retention is for several years, may impose no intolerable burdens. The volume of e-mail may well fit comfortably on computer hard drives, and complex searches to retrieve old e-mail -- far less likely for these organizations than for larger and more complex organizations -- will be similarly manageable.

For large and complex organizations, single period, uncategorized retention without some sort of winnowing process is not likely to prove a viable option. A very large organization may well

generate and receive hundreds of millions or billions of e-mails a year, and almost certainly will, in the course of this activity, create and receive e-mail with a high degree of legal and operational importance. If the organization is a multi-national, at least some of it is likely to be subject to laws requiring its mandatory retention for a significant period of time. Retention of all e-mail for five, ten or more years, with all of the attendant costs for infrastructure and hardware may be prohibitive; and searching such a monstrous collection of e-mail with anything approaching thoroughness may be impossible. On the other hand, sorting and indexing of that same collection of e-mail for retention purposes will be equally daunting. The magnitude of the problem rises with the size, complexity and legal environment of the organization in question.

Larger, more complex, highly-regulated or high-risk organizations may therefore be faced with a choice as to how granular and complex to make any e-mail capture scheme. Mirroring a paper-based file plan in the e-mail system may be prohibitively expensive or impossible to implement; insufficient granularity may result in lost legal disputes or outright violations of law. Some simplified version of the paper system, with an associated simplified version of the retention rules, may either be a satisfactory resolution of the cost/benefit equation, or the only practical option available. There are no fixed categories of organization or set analytical criteria that permit blanket application of any theoretical set of rules; in the final analysis, how much granularity and complexity is enough is a judgment that must be made based upon an analysis of the organization in question; its needs, its budget, its risk tolerance, its ability to implement a given solution and many other factors.

7.6.2. Electronic versus Paper-Based Retention

For small organizations or organizations with simple needs, retention of e-mail as printouts or word processing files may be a completely satisfactory solution. Such organizations may also be completely satisfied by a simple electronic scheme involving creation of multiple e-mail folders and drag-and-drop implementation by users, including manual implementation of simple retention rules. Larger and more complex organizations are likely to find such solutions less satisfactory. Properly implemented and enforced, such solutions impose no theoretical barriers to effective e-mail management. Consistent implementation of them in a large-scale and geographically diverse environment may nevertheless prove problematic. However, if the funds and willpower are not available for purchase and implementation of what may turn out to be a large and complex technology solution, printout or drag-and-drop retention may be the only options available.

For organizations in highly-regulated or very high-risk environments, complex and granular indexing via sophisticated software tools, and/or the imposition of rigorous and heavily enforced management rules, may be the only realistic option, regardless of the costs associated with them. Regulators and other authorities can and do demand e-mail, and penalties for failure to produce it can be very high indeed, including as they do the potential for very serious criminal charges if there is an appearance that the e-mail not produced was purged to hide evidence of misconduct. Although this does not preclude a paper-based e-mail retention system, any such system would likely have to be integrated with search tools in the form of indexing schemes or software to permit management and search capability sufficient to respond to severe regulatory requirements

and litigation demands. Meeting those demands might be beyond the capability of anything but a very sophisticated and fully searchable e-mail management system.

8.0. A Final Word

Lack of an ideal solution applicable in every instance forces any organization contemplating e-mail management into an analysis of its own needs and characteristics. In the absence of sound information on these matters, any solution -- or as often will be the case, combination of solutions -- will be less satisfactory than it might be.

Some of this analysis and implementation need not be made on a high level within the organization. It is not normally the case that granular central control of files extends to individual file drawers on desks or to individual hard drives on computers; rather, organizations more typically impose high level rules of governance, and boundaries that should not be crossed, combined with some lesser degree of central control at the local level. Within the rules and boundaries, operating units and other entities within the organization are free to impose low-level solutions that are operationally efficient and administratively convenient. The reason that detailed control is devolved upon individual users or departments is a simple and sound one: the centralized controller is likely to have far less understanding of the operational needs of the user, and of the resources available to meet those needs, than is the user themselves. For many organizations, the rules-and-boundaries approach -- which may well result in a combination of approaches and solutions -- may prove the most effective solution.

In *Public Citizen v. Carlin*,[126] this question was placed squarely before a reviewing court in the public records context. In the explanatory remarks accompanying publication of an e-mail retention policy, the Archivist of the United States stated:

> "Agencies must maintain their records in organized files that are designed for their operational needs. Agencies that currently have traditional paper files print their electronic mail records, word processing records, spreadsheets, and data base reports so that their files are complete, comprehensible, and in context with related records. Agency functions that have not been automated must be supported by hard copy files, even when some types of related records are generated electronically. Agencies that decide to maintain their records in electronic recordkeeping systems do so for compelling operational needs, not for future researchers. In some cases ... agencies create automated indexes to hard-copy records rather than digitizing all of the records themselves. In any case, the decision must be based on an analysis of the needs of and benefits to the agency, balanced against available resources."[127]

[126] *Public Citizen v. Carlin*, 184 F.3d 900 (D.C. Cir., 1999).
[127] Explanatory notes to *General Records Schedule 20; Disposition of Electronic Records*, 60 Fed. Reg. 44,643 (1995) at 44,644/1-2.

In reviewing this and other justifications of the policy, the appellate court said simply: "[W]e think this decision to permit agencies to maintain their recordkeeping systems in the form most appropriate to the business of the agency is reasonable."[128]

This common-sense explanation and response provide both the authority and a solution for many organizations, large and small.

[128] *Public Citizen v. Carlin*, slip opinion at II (b)(B)(1).

Funds for this study were provided by

The ARMA International Educational Foundation

The ARMA International Educational Foundation is the non-profit, (501(c)3, affiliate of ARMA International, the primary professional association for the records and information profession in the world.

Mission
The ARMA International Educational Foundation supports education and research initiatives that promote the advancement of both information managers and the information management profession. Recorded information is the lifeblood of the modern organization, but rarely is it treated as a critical asset, primarily because there is little quality research to create the comprehensive body of knowledge required to support information management as a profession. The AIEF purpose is to answer that need by soliciting funds for this research and then providing a vehicle through which conclusions can be tested, documented and communicated to the information management community.

If you found value in this publication, please consider making a financial contribution to the Endowment Fund of the Foundation. This can be accomplished by visiting the Foundation's web site, www.armaedfoundation.org, or by contacting

Foundation Administrator
ARMA Int'l Educational Foundation
1609 Terrie Drive
Pittsburgh PA 15241
USA

Additional information about the Foundation can be found at GuideStar

The National Database of Nonprofit Organizations
http://www.guidestar.org/search/report/gs_report.jsp?ein=31-1556655

Comments about this publication and suggestions for further research are welcome. Please direct your inquiry to the Foundation Administrator.