

It's 10 O'Clock: Do You Know Where Your Records Are — And What They Are Doing?

Remarks by Patrice McDermott, OMB Watch
FIRM Council Summit
16 November 99

Thank you for inviting me to speak today. I am sure that the name of my organization — OMB Watch — already puts me on good footing with most of you and I am pleased to talk with you on the critical subject at hand.

In 1982, the Committee on the Records of Government proclaimed that "the United States is in danger of losing its memory." ¹ Earlier this year, at an American Association of Law Libraries meeting, Scott Armstrong stated that he is "reconciled" to the loss of 20-plus years of the history of our federal government. [Anyone who knows Scott knows—thankfully, from my perspective—that he is not *really* reconciled, but that is not the point here.] And, of course, this is not just the loss of our family photos, as it were, but of that information necessary for accountability that makes this a profound concern for all of here in this room. What brings all of us together in FIRM (and I say "us" because I am a participant) and together today is our shared concern—indeed anxiety—about the state of our nation's electronic records.

At the risk of repeating what you already know, let me start with what we are talking about here. We tend to think that when we create a document—electronically or otherwise—we create a record. But that is not true. We, using computer systems, do not *per se* create or maintain *records*—specific intervention and planning is required to ensure that the essential characteristics of the record are built into information systems—electronic or paper—and maintained. These essential characteristics are content, structure, and context. For paper records, all of these elements are contained within the same physical medium—the sheet of paper and the attached sheets. The content characteristic is obvious; a form is readily distinguished in its structure from a report; the context can be gleaned from the address and salutation, the signature line, the cc's, the date, and so on. The context in terms of provenance—or chain of custody—can be ascertained from the file codes, charge-out forms, etc.

In the electronic world, the only *approximate* match is with the content. Even here, however, this apparent match is deceiving. We think (if we think about it at all) that when we type in letters from our keyboards, they are converted into a universally shared standard code—ASCII. I will leave aside all the problems associated with the difficulties this code presents for sending diacritic characters electronically [and any of you who have tried to send or receive non-English words over e-mail will know exactly what I am talking about], even ASCII is not completely standard—IBM has its own EBCDIC character encoding scheme, and Apple and Intel-based PCs each differ in the ways they support extended ASCII character sets. So, there is one problem. With just straightforward *text*.

But, other than e-mail, most of us don't create documents in straight ASCII text. We create them in word processing or desktop publishing systems that embed complex structure and layout elements into these documents—and these elements are typically in proprietary terms. All of us, I am sure, have had experience with "converting" a Word document to a WordPerfect document with the attendant loss of content such as page structures and the layout of headers, footers, etc.

So, even the apparent equivalence of content in paper and electronic formats is far from simple and transparent. And this does not even begin to get at structure and context.

Terry Cook has given an example of a CEO who sends a message out electronically. As he notes,

the interconnections of her compound message are not part of what the user sees on the screen—the rough equivalent of our paper document—but are, rather, links in software or in the operating system. "These instruct the computer to query the database, drop the relevant values found there into a spreadsheet, build a graph using spreadsheet formulas, and place the resulting graph in the appropriate spot in the word-processed report that is attached to the e-mail." As Cook notes, no such product is actually stored anywhere in the computer: "upgrade or change that software or system, alter any of the data values, and those relationships among the e-mail, report, graphic, spreadsheet, and database are lost.... The virtual document vanishes. Corporate memory is wiped clean."²

Indeed, for any document stored and shared digitally, users operate on exact *images* of the original works stored in their local computers. This enables multiple, possibly simultaneous uses from a single original. The technology creates great opportunities for collaboration and for editing. It also creates great challenges for records management and for archiving. A project led by Richard Cox, Richard Bearman and John McDonald has determined three essential needs for capturing, maintaining and using electronic records³:

- **Comprehensivity**—a record reflecting who, what, when, where, why, with whom, and so on, must be created for every government transaction. Records cannot be created for some transactions and not for others if the trustworthiness of the institution's record-keeping system is not to be thrown into doubt and its value as evidence considerably weakened.
- **Authenticity**—authorizations for access to data, or parts of it, must be recorded, and traceable to each record and transaction. Verifying what was sent, seen, received, and deleted by whom requires capturing in the electronic record the kind of security controls that already exist for paper document—or the overall context of the communication is lost.
- **Fixity**—records must be tamper-proof—no deletion or alteration to a record should occur once the transaction to which it relates has taken place. If a record is changed, or corrected, a second record must be created and linked to the first. Moreover, each use—viewing, indexing, classifying, filing or copying of a record is also a transaction and thus must generate its own record. This makes it possible to know on which records decisions were based. It is impossible for this to happen unless there are indexing and searching mechanisms in place in the system and these are captured for the time each decision was made.

Of course, this list does not answer the fundamental question of which of the electronic documents is the record, when, and whose is the responsibility for its designation and maintenance.

As if all of this were not daunting enough, what is on the very near horizon (if not already here in many instances) are interactive electronic forms on the Web, digital signatures — encrypted or key infrastructure, multi-format documents [how do you handle an interactive Web video conference?], and so on. The issues with the banking bill around electronic notification and related concerns is just the tip of the iceberg. The issues raised there did not concern the issues raised in other venues about online security — which is central to the authenticity and fixity of the record.

And none of this gets to the fundamental point for each of our discussions here today—access. If the *documents* of our government are not being made into *records*—and there is general apprehension that the necessary specific intervention and planning mentioned earlier is not occurring—there is no real possibility for meaningful access over time for you or for the public. We will none of us know where our records are nor what is happening to them and their meaning.

You are here and part of this organization because you understand that acknowledging and taking responsibility for the government's electronic records cannot slide any longer. Scott Armstrong and others note that the government began to move into the digital world at least 15 years ago. As we have learned, the problems have not become *less* complex nor the solutions easier. They are assuredly not going to turn in that direction now. What is needed is the work you are undertaking—but also leadership and commitment from the policy makers to move the organizational cultures to make the changes that have to be made to ensure the creation of electronic *records*, their maintenance over time, and their usable accessibility by those who want to know what our government has done and is doing.

Thank you.

- 1 . Committee on the Records of the Government 1985:9, 86-87.
- 2 . Cook, Terry. "It's 10 O'Clock: Do you know where your data are?"
<http://www.techreview.com/articles/dec94/cook.htm>
- 3 . In Cook, *op cit.* p. 5 .