KAHN
CONSULTING INC.

Missouri Electronic Records Education and Training Initiative

Electronic Records: Legal Challenges and Issues

Barclay T. Blair
Director, Technology Practice
Co-Author, "Information Nation"
bblair@KahnConsultingInc.com

I. A New Era for Records Management

What is Happening Out There?

"Instead of obtaining a copy of all e-mail files, county staffers suggested that residents would need to sit at each official's computer and manually check the e-mail received."

County Can't Deliver Email to Public, St. Petersburg Times

What is Happening Out There?

- City Plans to Archive Email
  - Fredericksburg Free Lance-Star, August 2003
- Meltdown at County Recorder's Office
  - Headliner News, August 2003
- Staff Grilled on Records Fray
  - Gurnee Review, October 2003
- FOI: E-mails Should Be Public
  - Record-Journal, October 2003

What is Happening Out There?

- E-Mail Gray Area of Virginia's FOI Act
  - Times-Dispatch, October 2003
- State Sued For Deleting E-Mails
  - Sacramento Bee, February 2003
- County Can't Deliver E-Mail to Public
  - St. Petersburg Times, September 1999
- Records Purged From Computer
  - Fayetteville Online, August 2003

Agenda

1. The Changing Landscape for E-Records
2. Legal Foundations
3. Classifying and Managing E-Records
4. Providing Access: Inspection, Examination and Copying
5. Public Records and Personal Privacy in the Email Environment

A New Era for Information Management

October 2001

"It might be useful to consider reminding the engagement team of our documentation and retention policy. It will be helpful to make sure that we have complied with the policy. Let me know if you have any questions."

Arthur Andersen Attorney Email

June 2002

Andersen found guilty of obstruction of justice. The firm is given the maximum penalty under the law, is no longer in the auditing business, and has lost tens of thousands of employees.

The Landscape Has Changed: Why

- The Securities and Exchange Commission fines five broker-dealers a total of $8.25 million for failure to preserve email communications.

- The US federal government finds that “records management guidance is inadequate in the current technological environment of decentralized systems creating large volumes of complex electronic records.”

The New York Times ON THE WEB

- A major federal agency notifies a flight school, six months after 9/11, that two of the 9/11 terrorists have been approved for student visas. The agency admits in 2002 that its “current system for collecting information is . . . antiquated, outdated, inaccurate, and untimely.”

- To recover records related to the Indian Reform Trust, it will cost 2.6 billion dollars (WSJ February 23, 2004)

THE WALL STREET JOURNAL.

The Landscape has Changed: Why?

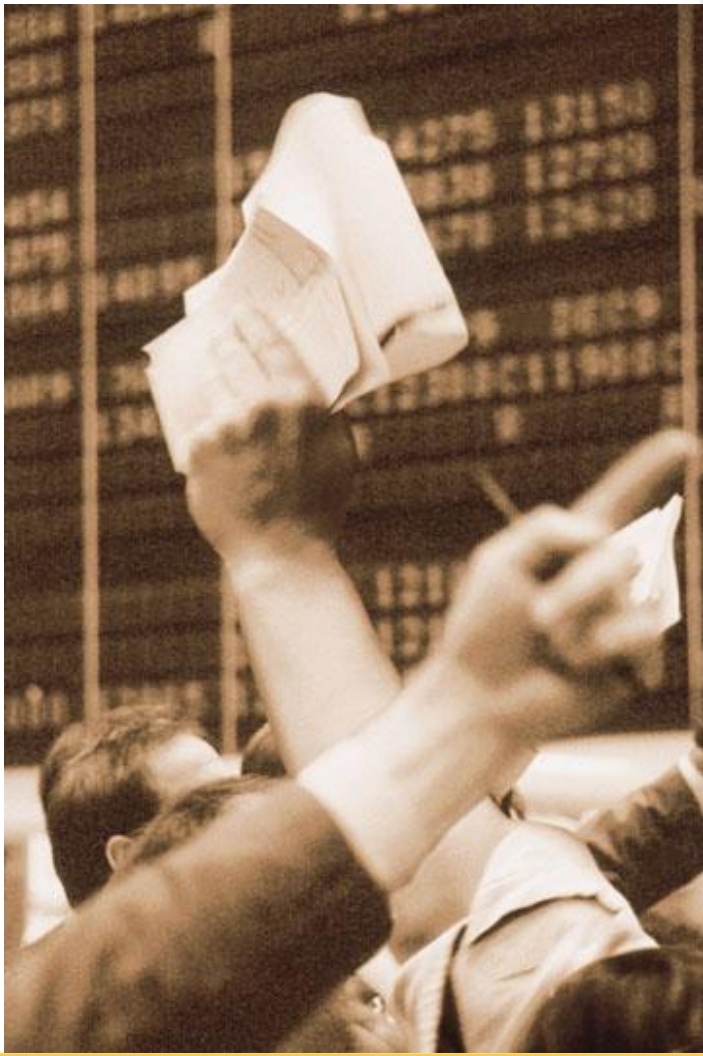
- In 2003, 800 megabytes of new information was created for each man, woman and child on the earth – with 92% of it stored on magnetic media, primarily hard drives. (UC Berkeley)
- Businesses worldwide today use more than 300 million desktop computers that together have the capacity to store 150,000 terabytes of information. (Storage Network World)
- The number of email messages sent per day will grow from 31 billion in 2002 to 60 billion by 2006. (IDC)
- Roughly 250 billion text messages were sent worldwide using wireless devices in 2001 (World Wireless Forum)
- Business users are expected to make up nearly half of the 500 million people that will be using instant messaging by 2006. (IDC)

What Has Changed?

- Properly managing records and other information has become inextricably linked with corporate accountability and transparency.
  - The bankruptcy of Enron alone is estimated to have caused $70 billion in wealth to vanish
- This in turn has become linked to fiscal health and stock market valuation.
- An era of new expectations, new regulations, new laws, new technologies, and new challenges.
- New awareness, emphasis.
- Increasing funding???

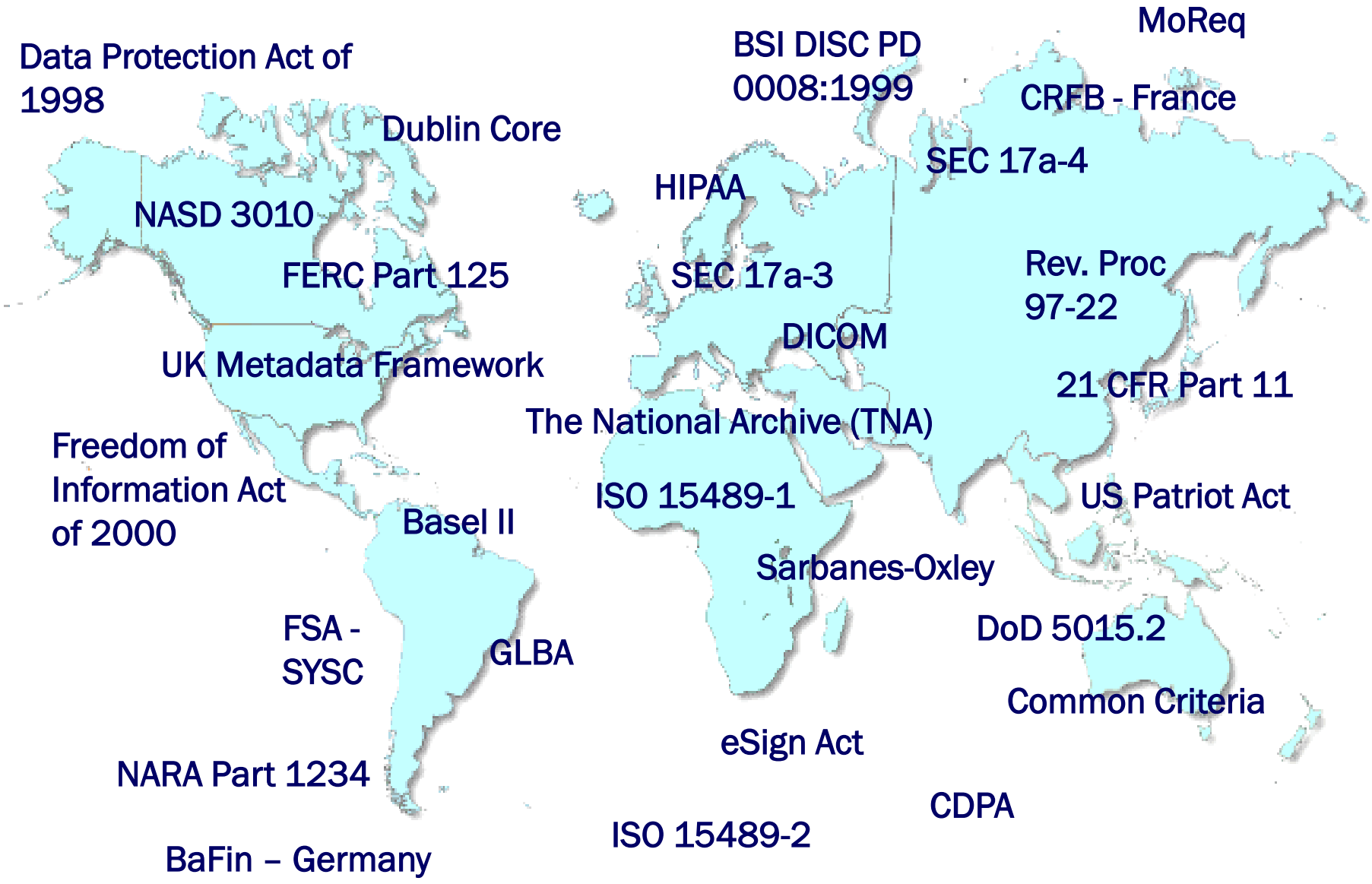
Why Have These Events Happened?

- The natural result of market cycles
- The rush to technology (State and local government spent $40.4B on IT in 2003)
- The design of information technology itself
- Authority and responsibility
- Lack of a holistic view



II. Legal Foundations

E-Records Laws and Regulations Across the Globe



Ongoing Evolution

- **1995**: Web-based E-Commerce emerges
- **1996**: United Nations Model Law on Electronic Commerce
- **1996-1999**: Several state digital signature laws introduced and enacted
- **1996**: HIPAA (Health Insurance Portability and Accountability Act)
- **1997**: FDA 21 CFR Part 11, SEC 17a-4
- **1998**: Government Paperwork Elimination Act
- **1998**: NASD 3010 Updates
- **1999**: Uniform Electronic Transactions Act (UETA) model law
- **2000** onward: International e-commerce legislation
- **2000**: Electronic Signatures in Global and National Commerce Act (E-Sign)
- **2002**: Sarbanes-Oxley Act
- **2003**: Important compliance deadline for HIPAA Administrative Simplification section
- **2003**: California Database Protection Act of 2003 (CDPA) (S.B.1386.3)

State and Local Government

- Public records laws
- Freedom of Information acts
- Open meetings laws
- Public access laws
- Records retention laws
- Etc.

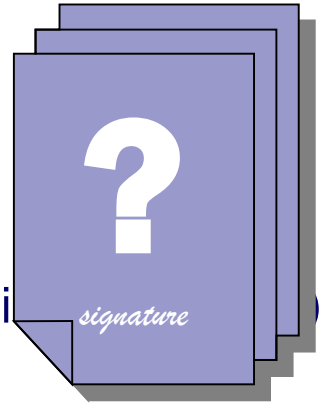
Where Are We?

- The statutes have been updated to deal with electronic records
  - Public and Business Records Law, Chapter 109 RSMo
  - Missouri Sunshine Law, Chapter 610 RSMo
  - Missouri Code Of Regulations
  - A record is any “document, book, paper, photograph, map, sound recording or other material regardless of physical form or characteristics made or received pursuant law or in connection with the transaction of official business.”
    - RSMo 109.200 – 510
- The law is still being interpreted and applied, and there is still a lot of work to be done

What Are These Laws Trying to Achieve?

Authenticity

- Can we prove or demonstrate:
  - Who or where it came from?
  - What role it had in a transaction or business activity?
  - When it was created?
  - Who had control of it, and when (i.e., “audit trail” or “chai
- In the paper world, common techniques include:
  - Printing processes (for example, anti-counterfeiting)
  - Letterheads and other legends
  - Postal marks
  - Handwriting analysis
  - Business process analysis
  - Handwritten notes (e.g., “clean up all documents” – Nancy Temple)



Confidentiality

- Can we protect the confidentiality of an email message?
- Well-understood and tested methods exist to ensure that unauthorized parties do not gain access to a document during transport or storage:
  - Couriers
  - Registered mail
  - Locked offices and filing cabinets
  - The envelope
- What are the equivalents in the digital world?

Nonrepudiation

- Will the signer of a document be able to claim that he/she did not sign a document?
- Repudiation of signed paper documents does occur, but not very often.
- Nonrepudiation is a quality that really results from the *entire* process, not a single element.
- However, signature cards, handwriting analysis, and the physical qualities of ink on paper are all used to prevent repudiation.

Document Integrity

- Can we demonstrate that a email message has not been altered since it was signed?
- The physical qualities of ink on paper are the biggest safeguard here – it is difficult to alter a paper document without detection
- Other techniques include:
  - Secure delivery and storage
  - Watermarks and seals
  - Careful management of drafts and copies

Signature Intent

- Does the electronic signature demonstrate the reasons that the document was signed?
- Documents are signed for many reasons:
  - demonstrating agreement
  - agreeing to be bound
  - showing an understanding about the subject of the record,
  - assenting to terms, etc.
- Contracts are often disputed over intent – a disputed lack of understanding, agreement, etc.
- The act of signing a paper form is familiar and culturally ingrained, so intent can often be inferred from the document and the context.

Permanence

- Can the email message be preserved in order to meet our legal, business and historical needs?
- Signed paper documents provide an excellent records of business activities that can last for decades, if not centuries, if properly managed
- No special technology or skill is required to read archived paper records

Signature Linkage

- Is the signature linked to the electronic document in a secure manner?
- This linkage is important to prevent the unauthorized use of a signature.
- A handwritten signature is inextricably bound to the paper form. It cannot be “removed” and used for unauthorized signing.
  - The complexity and uniqueness of a handwritten signature is a barrier to unauthorized use

Legally-Recognized Record

- Can the email message be used as a legally-recognized record of a business activity?
  - The law recognizes signed paper documents in virtually every jurisdiction worldwide.
- All critical information pertaining to a signed paper form exists within the “four corners” of the document
  - Legal practice for collecting and presenting this type of evidence are well established

Trustworthiness: What We Are Trying to Achieve

1) **Integrity.** No alteration. Complete from creation to disposition.

2) **Accuracy.** Contains what it is supposed to contain, as originally intended, and the content remains the same over its entire lifecycle.

3) **Authenticity.** Source or origin can be reliably demonstrated. This often requires proof of who generated an e-record, and who controlled it over its lifecycle (often called an "audit trail).

4) **Accessibility.** Accessed in a timely fashion during its lifecycle precludes its use for these purposes. Accessibility can be threatened by poor indexing, the finite life span of storage media, hardware obsolescence, software incompatibility, environmental degradation, and many other factors.

Challenges to Trustworthiness

- **Complexity.** Understanding the creation of a paper record is usually straightforward. Many e-records, however, are created using complex technological process that may be hard to explain to a court or regulator, which can add to the time and expense of presenting complex electronic evidence.
- **Portability.** E-records can be easily created and distributed, which can make it more difficult to track their origin and use throughout their life span.
- **Alterability.** Unlike the physical bond of ink on paper, most e-records provide no such inherent characteristics that prevent their inadvertent or deliberate alteration—even though certain storage technologies can prohibit unauthorized alteration or deletion.
- **Hardware and Software.** E-records rely on hardware and software for their display and use—hardware and software that may not always be available.
- **Multiple Parts.** Paper records contain all of their information within the "four corners" of a document. E-records, on the other hand, can contain metadata and exist in multiple parts in multiple locations – thus making their capture, retrieval, and presentation more problematic.

Risk Category

Level of Risk	Relationship Between the Parties	Transaction Value	Future Need for Accessible, Persuasive Information on the Transaction
Low	Intra-Agency	Transactions where no funds are transferred, no financial or legal liability is involved and no privacy or confidentiality issues are involved (electronic signatures are least necessary in these transactions and should not be used unless specifically required by law or regulation).	Transactions where the information generated will never be needed again.
Low to Moderate	Inter-Agency	Transaction fulfills a legal duty enforced by criminal or civil liability.	Transactions where the information generated may later be subject to audit.
Moderate	With Agency in another level of government (i.e., federal to state agency, state to state agency)	Involving information protected by Privacy Act or other statutes required restrictions	Transactions where the information generated may later be subject to dispute by one of the parties (or alleged parties) to the transaction.
Moderate to High	With a private organization or individual with whom the agency has an ongoing relationship	Involving contracts or commitments giving rise to financial or legal liability	Transactions where the information generated may later be subject to dispute by a non-party to the transaction.
High	One-time transaction with a private organization or individual	Involving transfer of funds	Transactions where the information generated may later be needed as proof in court.

Assessment Model adapted from OMB Guidance on federal agencies implementing GPEA

Practical Issues

- Capturing the right record during creation
  - A “clear & conspicuous” privacy policy
  - Database data vs. document or record
- “Admissible” does not mean “acceptable” or even “credible”
- E-Records laws are generally very accommodating from a technology perspective
- ESIGN/UETA:
  - “accurately reflects the information set forth in the contract or other record,”
  - “remains accessible” for the period the law requires
  - can be “accurately reproduced” in the future.

Practical Issues

- *"The management of e-mail systems touches nearly all functions for which a government agency is dependent on recordskeeping: privacy, administration, vital records management, administrative security, auditing, access, and archives. The need to manage e-mail messages and systems properly is the same as for other records keeping systems--to ensure compliance with California laws concerning the creation of, retention of, and access to public records."*
  - State of California Electronic Records Management Handbook

E-Records Challenges for State Government

- Retention and access may be harder to guarantee.
- The volume of information is itself a threat.
- New types of records are created.

III. Classifying and Managing E-Records

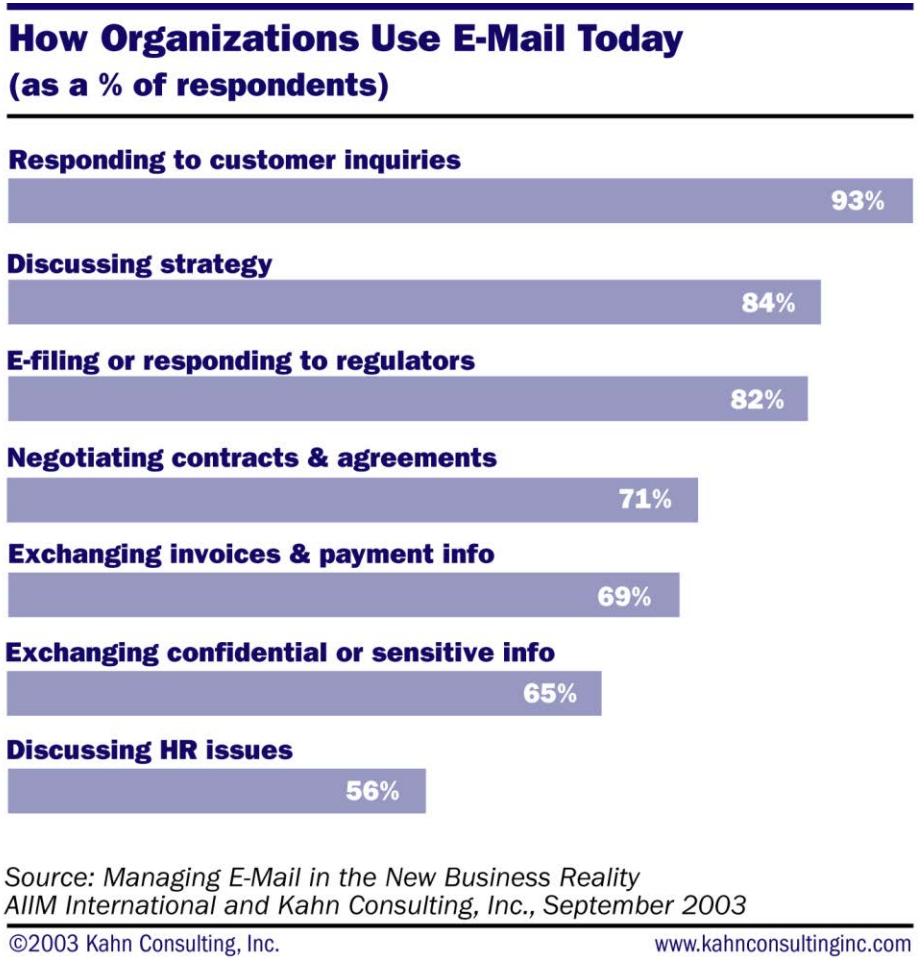
IT Challenges

"When agencies decide to upgrade or obtain a new computer system, they're looking at the most effective way to process and store knowledge. The demands of the public records law aren't generally considered early during the process."

"County Can't Deliver Email to Public,"
St. Petersburg Times

Email Alone is a Massive Problem

- E-mail volumes are increasing, but so is the value of the information in the e-mail system
- More messages that ever before have potential legal, compliance, and business significance and may have to be retained
- E-Mail today is about more than just lunch appointments - it contains records, private information, and potential smoking guns



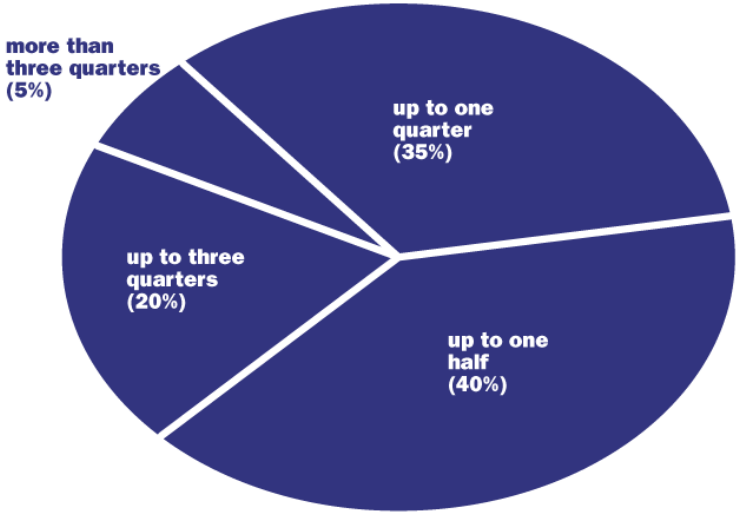
How Users View E-Mail

Popular Perception of E-Mail
(as a percentage of respondents)

Source: Managing E-Mail in the New Business Reality
AIIM International and Kahn Consulting, Inc., September 2003

www.kahnconsultinginc.com ©2003 Kahn Consulting, Inc.

Daily Time Spent on E-Mail Tasks
(as a percentage of respondents)



Source: Managing E-Mail in the New Business Reality
AIIM International and Kahn Consulting, Inc., September 2003

www.kahnconsultinginc.com ©2003 Kahn Consulting, Inc.

- 74% still see e-mail in a positive light . . .
- . . . even though 65% are spending more than a quarter of their day on e-mail tasks, and half receive more than 40 messages/day

Classification and Management

- State governments have unique classification needs
  - Driven by mandate to provide public access to records, while withholding certain records
- Solutions may be hard to find
- Needs may be different on an IT level than private enterprise, and specific solutions should be sought
- Let's examine these needs

Take Action: #1

- **Classify records when they are created.**
  - State governments that fail to adequately classify and otherwise identify public records at the time of their creation and/or retention and storage are inviting expensive problems down the road.
  - Up-front classification can minimize the impact of broad public records requests by making the retrieval of relevant records faster and more accurate.

Take Action: #2

- **Provide ready access to redacted records.**
  - Documents and other records often contain information that is subject to public access and information that is exempt.
  - State governments require systems that allow records provided for public inspection or copying to be redacted in a manner that protects the integrity of the original and ensures that protected information is not revealed.
  - Certain types of records, such as databases, and data streams generated from online transactions, may be difficult to properly redact and specialized tools for doing so may be required

Take Action: #3

- **Classify information that must be publicly accessible, but for which special procedures for access may be required or advisable.**
  - This includes information regarding public utilities and other infrastructure that is subject to public records laws but which also raises security and other important concerns.

Take Action: #4

- **Classify information that may require case-by case review.**
  - Some state public records laws require case-by-case review of information before it can be released to the public.
  - For example, until recently in Wisconsin, requests for most of the records within the personnel files of public employees could not be released before the employee was notified.
  - Classifying such information can speed the process of review and expedite the public access request.

Take Action: #5

- **Provide cost-effective copying capabilities.**
  - State governments have a mandate to provide citizens with copies of public records at reasonable cost.
  - This mandate can only continue to be fulfilled in the digital world if state governments have tools which allow them to cost-effectively retrieve and provide full and accurate copies of electronic records required to be released.

III. Providing Access: Inspection, Examination & Copying

Providing Access to Records

- May be flexibility in meeting the requirements, but a key requirement for all systems
- North Carolina's Public Records Act (G.S. § 132): "no public agency shall purchase . . . any electronic data-processing system for the storage, manipulation, or retrieval of public records unless it first determines that the system will not impair or impede the agency's ability to permit the public inspection and examination, and to provide electronic copies of such records."
- Illinois requires adherence to industry standards for e-records management systems AIIM TR31-1992)
- California: agencies are provided with detailed guidance on the selection, configuration, and management of government email systems, including the requirement that such systems "should retain all data and audit trails necessary to prove its reliability as part of the normal course of agency business," and that "the record copy of a message is identified and maintained appropriately."

Search and Retrieval

- All organizations struggle to find e-information, but in often politically-charged state government environment, search and retrieval takes on unique dimension
- Iowa Open Records law case
- State governments struggle to respond to requests for email and other electronic records in a timely, cost-effective, and comprehensive manner.
- As email use and volume continues to grow, the problem is likely to only get worse before it gets better.

"Department officials say that . . . email wasn't turned over . . . because the agency didn't have a system in place to uniformly search electronic files."

"E-mail Retrieval to Cost State Unit $10,550"

Des Moines Register

Methods of Access: Onsite Computers

- Is providing an onsite computer a solution?
- Topeka, Kansas case
- Providing open access to information systems is a bad idea

"According to the survey, [a state official] swore at [the] student . . . when she requested public records. The survey also said [the official] grabbed her arm and threatened to call police."

"Few Connecticut State Agencies Comply With Records Laws," Associated Press

Methods of Access: Onsite Computers cont'd

- **Segregating public records access terminals and systems.**
  - Access should be limited to separate, self-contained systems that contain copies of the public records redacted as required.
  - The separation of public access systems from mainline system will help to prevent the authorized access of non-public records and protect operational systems for possible corruption and performance degradation due to malicious or inadvertent acts of those using the terminals.
- **Limit searches.** Limit the ability to search records on the public terminals only to those records the public are entitled to view.
- **Protect from alteration.** Where possible, present records using images, encryption, or other technology that can work to prevent the unauthorized alteration of records.

Methods of Access: Controlling Fees

- Must strive to control the costs related to searching and copying records.
- While the amount that can be charged for copying records is often controlled by law (especially in the case of court records, for example), some jurisdictions charge varying amounts for the same service.
- A recent study in Montana found that fees varied wildly, from 15 cents for a page of city council minutes in one county, to $5 per page for sheriff's office incident report in another.
- Consistent procedures and technology platforms can help to ensure that the cost of providing copies and related services is minimized and is relatively consistent.

"The lawsuit . . . claims the county's new method of making records public over the Internet restricts dissemination of those documents."

"Public Records Case Set for Nov. 3 Trial," Hollister Freelance News

Methods of Access: Accountability

- California Database Protection Act: A sign of things to come?
- Response to massive hacking incident in state government agency
- Any “state agency, or a person or business that conducts business in California, that owns or licenses computerized data that includes personal information” to notify California citizens if their personal information is “acquired by an unauthorized person.”
- Affected parties may bring civil actions to recover damages.
- This law clearly highlights the need for state agencies to have adequate policies and procedures in place for protecting private citizen information.

Methods of Access: Consistency

- State and local governments need to ensure that paper and electronic records are being managed consistently, and that retention rules are followed regardless of where records reside or the medium upon which they are stored.
- *State ex rel. Dispatch Printing Co v. City of Columbus*
  - Inconsistent application of policy to paper and electronic records
  - 10 years of electronic records were found and made available

III. Public Records & Personal Privacy in the Email Environment

Email Must Be Managed

- Email provides benefits
  - Can speed decision making
  - Increased citizen communication
- However, email is also used casually
- As a result, personal and public records are often intermingled in the government email system
- What is the boundary between the two - how do the courts decide?

"E-mail may include transmissions that are clearly not official business and are, consequently, not required to be recorded as a public record."

State v. City of Clearwater, 2003 Fla. LEXIS 1534 (Fla., 2003

Do Organizations Get It Yet? Email Policies

- Nearly every organization has got the message they need to control employee e-mail use
- Several e-mail policy elements are common
- However, organizations are failing to take control of the “next big” issue - e-mail retention
- There is a great deal of confusion out there:
  - 25% - retain more e-mail
  - 31% - retain less e-mail
  - 21% - longer retention
  - 30% - shorter retention

- Despite what policies might say, only 37% use e-mail content as a retention criteria

Just What is a "Personal" Email Message?

- Arapahoe County, CO case
  - public records include "the correspondence of elected officials, except to the extent that such correspondence is . . . without a demonstrable connection to the exercise of functions required or authorized by law or administrative rule and does not involve the receipt or expenditure of public funds . . . ."
- Although intimate, the "e-mails involve[d] the expenditure of public funds, and thus, are public records subject to disclosure under CORA."
- The court made this determination because:
  - the email messages were sent while the individuals were working;
  - were sent over a county email system for which the county paid monthly fees to use;
  - and were sent over county-owned pagers - all activities that incurred the expenditure of public funds.

Take Action: #1

- **Policies.**
  - Implement and enforce email policies that minimize the use of the email system for personal use and provide directives on the type of content that is appropriate for email messages. Tools such as content filtering can assist in controlling inappropriate content.

Take Action: #2

- **Classification.**
  - Limit the use of the email system for transmitting private, confidential, and other information that the public may not be entitled to access.
  - Alternatively, employ tools that will allow employees to easily designate and classify email messages that contain information that is covered by an exception.
  - These strategies will help to minimize the cost of fulfilling FOIA requests and of records management obligations generally.

Take Action: #3

- **Establish formality regardless of the size of government.**
  - In small counties and towns there may be less formality in the way that email is used and managed.
  - In Fredericksburg, Virginia, “most members of council use their personal e-mail accounts, rather than the ones set up by the city, to receive and send electronic communications about council issues.”
  - That is, until, a massive FOIA request required the City Clerk to spend a week sorting through 5000 email printouts spread throughout her home, trying to determine which messages were relevant to the request.
  - While the cost of using email may seem insignificant, the cost of complying with access requests can result in significant unbudgeted expenses.

Take Action: #4

- **Establish rules for email devices.**
  - Email increasingly resides in multiple locations, including mobile devices.
  - PDAs and other devices designed to send and receive email and keep schedules are likely to contain both personal and government-related information.
  - It is increasingly likely that the information contained on such government-supplied or supported devices could be included in public access requests - creating further headaches for administrators charged with assessing privacy issues

Case In Point: The Used BlackBerry

The Situation

- In 2003, investment banker's Blackberry bought on EBay contains hundreds of sensitive e-mails and thousands of contacts
- Misuse of information by buyer could have led to contract violations, regulatory action, espionage, and HR problems
- Seller thought removing battery erased information - device was not erased by employer

Implications

- Enormous loss can happen with the smallest devices
- Use proper and consistent decommissioning of devices
  - Apply to all employees
  - Watch for "rogue" ownership and control by policy
  - Empower IT and HR to enforce policy

Information Found:

- A database containing the contact information (in some cases, even home phone numbers) of more than 1,000 of the bank's employees, including senior executives

- About 200 internal company e-mails that revealed information such as loan terms for various investment bank customers, non-public information about mergers and restructuring, and discussions with a customer about whether or not they should strictly adhere to the terms of contract

Conclusions

- Failing to retain, preserve, and make available the records of government, even if in email form, undermines the foundation of good government: transparency and public trust.
- State governments face many unique electronic records management challenges.
- In the face of the growing volume and value of email and other forms of electronic records, these challenges are only increasing.
- Act today to ensure that plans to deliver government services electronically and conduct business using email and other digital communications technologies are backed up by legal work.
- Failing to do so will only increase the costs and disruption that will inevitably result in the future.
- Acting proactively will diminish the likelihood of future problems and allow governments to take advantage of operational efficiencies that result from information and records management activities

Missouri Electronic Records Education and Training Initiative

Questions and Discussion

Barclay T. Blair
Director, Technology Practice
Co-Author, "Information Nation"
bblair@KahnConsultingInc.com
250-686-9619

KAHN
CONSULTING INC.