

Personal Information Protection, Privacy and Legal Admissibility of Electronic Documents, Records & Images



Compliance To Standards and Legislation

Michael Bookbinder

Interactive Technologies International

michael@itiinternational.com/ www.itiinternational.com

(905) 689-4838

Challenges for Information Lifecycle Management & Compliance

- Mergers and Acquisitions
- Merging of personal information
- Personal information left on PC drives
- New products
- New business entities (some virtual)
- New Alliances.....and
- New Risks:
 - Privacy issues
 - Security and control
 - New legislative and regulatory environments

Privacy

- Privacy has several dimensions:
 - Protection of personal data, or informational privacy or data protection.
 - Personal data not to be automatically made available to other individuals or organizations without their consent
 - Data held by another party, the individual must be able to exercise a substantial degree of control over that data and its use.

Privacy vs Confidentiality

- Privacy is often confused with confidentiality
 - Confidentiality refers to the duties or obligations of individuals and organizations to safeguard the information they have been entrusted with.
 - Privacy is:
 - The right to be left alone
 - Free from interference by others
 - Protection of personal information

Security and Privacy

- Security” and “privacy” often used interchangeable
- Closely related, but two different concepts
 - Security is all the steps a business or government might take to protect its functions and assets
 - Privacy is a promise that governments and businesses make to citizens and consumers
 - Security allows privacy promises to be carried out, but the two are not the same

Changing Business Model

- Accounting scandals, the growing number of regulatory mandates, legislation and the litigation consequences associated with those regulations have prompted many businesses to bring compliance initiatives out of the back office and into the boardroom.

Governance, Accountability, Privacy Compliance

New Era of Corporate Information Access and Retrieval

- Board of Directors
- Executive Team
- Legal
- Internal and External Audit
- Regulators
- External Legal Counsel
- All employees
 - IT, RM, bus dev, marketing and other staff

What do we mean by compliance?

- “Compliance” is conformity with some criteria
- Complying with government legislation, directives and regulations requires:
 - Written and implementation of policies and procedures
 - Design and implement document and records processes and practices (classification, retention, disposition, destruction)
 - Include sound procedures for protection of privacy and security to protect integrity of information contained in the records and business systems
 - Ability to prove authenticity throughout the “Information Life Cycle”

The Business Benefits of Compliance

- Compliance allows companies to turn ongoing processes into their normal course of business.
 - Compliance provides the necessary foundation for storing, managing, processing and tracking of personal information and content in a central, secure repository for only those authorized to access them
 - Integrity and Authentication with effective storage management of the massive amounts of content involved in compliance documentation and records

Compliance Requirements Has Common Threads (Privacy & Governance)

Do one you get both!

- Impose New Policies, Procedures, Protocols and Responsibilities
- Not Just an Individual But Team Responsibility
- Personal Responsibility
- Organization-wide
- Security to Protect Assets and Guarantee Integrity
- Limit Liability
- Confidentiality

Compliance Requirements Has Common Threads (Privacy & Governance)

Do one you get both!

- Enhance Corporate Governance
- Accountability
- Accessibility
- Auditability
- Reliability
- Integrity and Authenticity
- Restricted Access
- Secure Storage - Retention
- Mitigate Risk
- Destruction According to Retention Program and
NOT Spoliation

Applications Requiring Compliance

- Content and Document Management
- Records Management
- Email Management
- Security
- Consent Management
- Privacy Management
- Business Process Management
- Storage Management
- Encryption
- Digital Signature
- Networking

Susceptible for Privacy & Discovery

If it exists, it is discoverable

- Active data
- Metadata
- System data
- Backup tapes
- Deleted files
- Legacy data
- Convenience copies

Regardless of Storage Medium, All Records Must be Destroyed According to Retention Schedule

Why be concerned about records?

- Personal information is contained within
- Privacy compliance needs coordination and planning between:
 - Information Technology
 - Records Management
 - Legal Counsel
 - Management (Team Work) & Executives
- Secure Storage is a key factor
- Records are being deleted without awareness or concern – i.e. backup tapes and Corporate official records

Why be concerned about records?

- Not many manage emails within a records management program
- Email not considered records for retention
- Lawyers and judges still not aware of electronic document and records systems

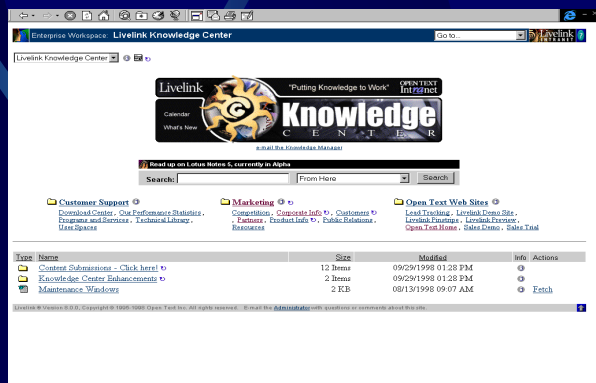
Secure Storage for Compliance

- Storage repositories used to hold digital information, content and records during their retention period
 - Adequate provision for the maintenance, preservation and confidentiality of the information and records
 - Not subject to unauthorized access and alteration
 - Content scan before unauthorized and noncompliant transmission of personal information
 - Ensure that digital content and records captured by the system cannot be lost or damaged through accident or omission i.e.
 - Disaster
 - Mischief
 - Accidental Erasure
 - Annotation or replacement not authorized

Content Management and Business Systems

- Personal Information and Business Records exist in:
 - Records (Evidence of actions occurring in the course of business)
 - Image of Research Papers, Application Form
 - Text of contract, Report, Manuals, P.O.s
 - Word Processing Documents
 - Video clips from interviews, Photographs
 - Spreadsheets
 - COLD documents
 - Computer Data
 - Voice Message, Instructions
 - Email, Faxes, Xrays etc...

Sources of Electronic Content, Personal Information and Data



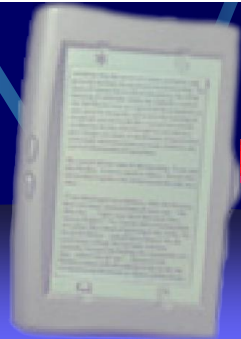
Web



Digital Camera



TVs, books, games

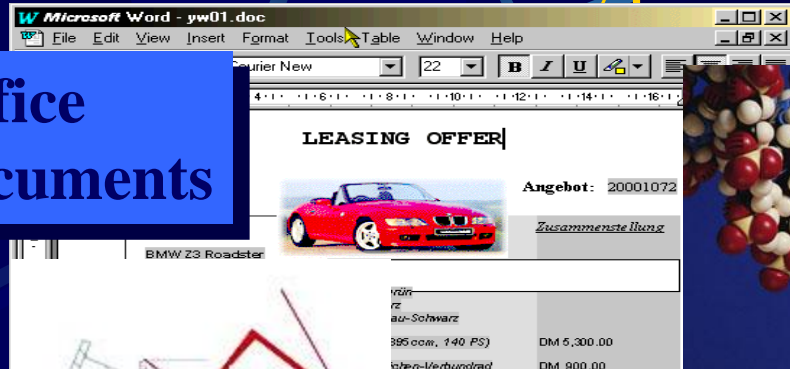


Phones, PC companions

Hand Held Wireless Devices

Privacy Infrastructures Must Support Restricted Access to a Range of Document Types and Formats

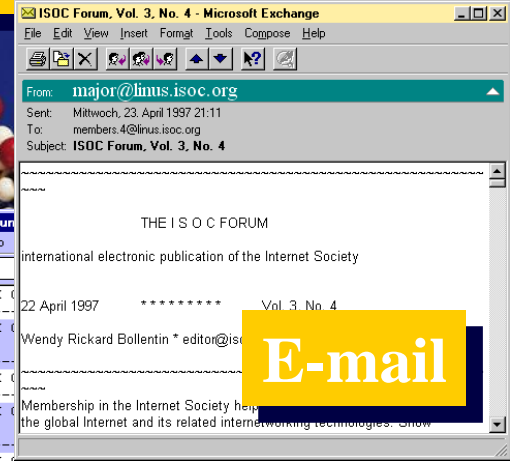
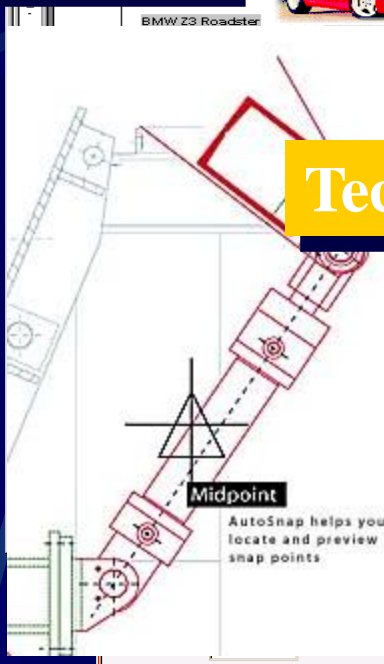
Office documents



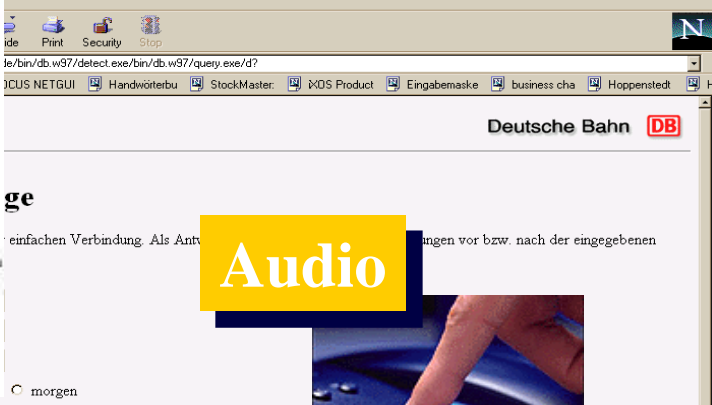
Digital images and video



Technical drawings



E-mail



Audio



COLD printlists

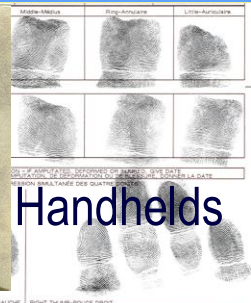
A table with columns for 'Sachkonten' and 'Debitoren'. The table contains numerical data and currency symbols.

Sachkonten		Debitoren	
Soll-Betrag in HW	Haben-Betrag in HW	Soll-Betrag in HW	Haben-Betrag in HW
000001000 31	133,00		(USD 87,75-)
000001000 31	15.076,92		

Web documents



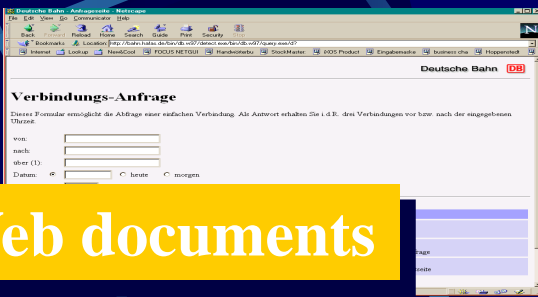
Handhelds



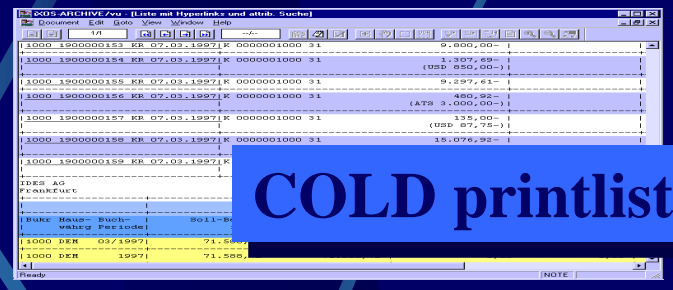
Personal Information Storage Media:



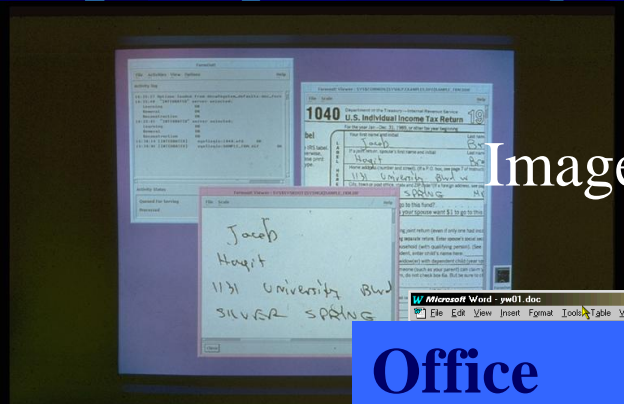
Paper



Web documents



COLD printlists



Image



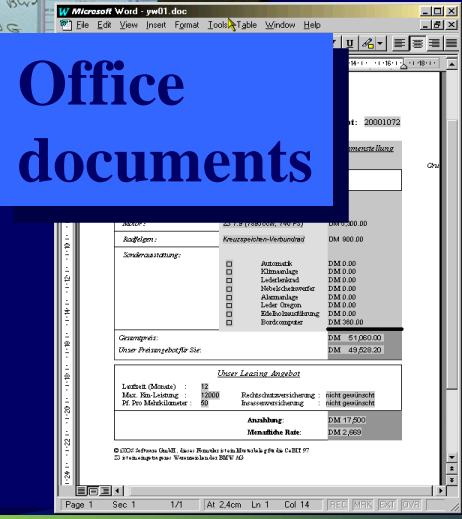
Storage



CD & Optical



RAID and Magnetic Storage



Office documents

Privacy & Personal Information Protection

Personal Information

- Includes:

- Name
- Address
- Gender
- Age
- Income
- Medical Information
- Transactional information
- Behavioral information
- Education
- Blood Type
- Marital Status, religion
- Race, ethnic, group, race, colour

The Personal Information Protection and Electronic Document Act – PIPEDA

PIPEDA - The Act in Brief

● PART 1:

- Organizations covered by the Act must obtain an individual's consent when they collect, use or disclose the individual's personal information.
- The individual:
 - May access personal information held by an organization
 - to challenge its accuracy
 - Personal information can only be used for the purposes for which it was collected
 - If an organization is going to use it for another purpose, consent must be obtained
 - Individuals should also be assured that their information will be protected by specific safeguards, including measures such as locked cabinets, computer passwords or encryption.

● PART 2: Use and acceptance of Electronic Documents and Records

● PART 3: Electronic Signature

PIPEDA Part II

- Must be able to prove the integrity of the system
- Must be able to prove the authenticity, integrity, reliability, accuracy and trustworthiness of the electronic information

Authentication of Electronic Documents and Records Part III

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.

Compliance Fundamentals

- Written authority from Sr. Management
 - Policy or by-law
- Program part of usual course of business
- Written authority on destruction of records
- Provision for systems and procedures
- Provision for quality assurance and audit trails
- Provision for security of system & records
- Must be stored in a “secure environment”

PIPEDA 10 Key Principles

- Accountability
 - Organization is accountable for personal information
 - Includes privacy point person, training staff, staff
- Identifying Purpose
 - Purpose of collection must be clear
 - Identify new purposes
 - Grandfathering issue
- Consent
 - Individual must give consent prior to collection, use and disclosure
 - Meaningful consent will depend on circumstances
 - Explicit and Implied Consent
- Limiting Collection
 - Collect only information required for identified purpose

PIPEDA 10 Key Principles

- Limiting Use, Disclosure and Retention
 - Consent required for other purposes
 - Destroy or anonymize information once no longer required
- Accuracy
 - Keep as accurate as necessary for identified purpose
- Safeguards
 - Protection and Security required
- Openness
 - Policies should be available and in clear language
- Individual Access
 - Information available upon request to correct errors
- Challenging Compliance
 - Ability to challenge all practices with PrivCom

ITI Professional Service Offerings

Legal Admissibility and Privacy

- Education and Awareness Briefings
- Requirements Assessment
- Compliance Analysis
- Policy and Procedure Write, Validate & Document
- Development/Write
- Monitor Compliance of Policies and Procedures
- System Audit
- System Certification
- Opinion Letter
- Performing Privacy Impact Assessments
- Consult with Corp. Management
- Organizational Needs Analysis
- Assess the Environment
- Certification
- Audit and Assist with Compliance
- Develop Communications Plans
- Deal with 3rd Party Partners and Contractors

Interactive Technologies - Michael Bookbinder
1 (905) 689-4838 www.itiinternational.com

Thank you