The SJR 38 Work Group on Identity Theft meeting January 9 at 9:30 a.m. in Room 102 of the State Capitol will address the following topics:

- privacy vs. right to know;
- data storage and disposal;
- 3rd party marketing; and
- followup responses to questions raised on security/credit freezes at the Dec. 9 work group meeting.

Relevant SJR 38 reference to privacy vs. right to know:

BE IT FURTHER RESOLVED, that the study review the various types of government records and the interaction between privacy and the right to know as these concepts affect the protection of identity, trade secrets, medical records, and other information regulated by privacy laws.

I. Background information on privacy vs. right to know (includes government records and trade secret confidentiality),

Constitutional Issues

Right of privacy, Article II, Section 10 of Montana Constitution:

The right of individual privacy is essential to the well-being of a free society and shall not be infringed without the showing of a compelling state interest.

Right to know, Article II, Section 9 of Montana Constitution:

No person shall be deprived of the right to examine documents or to observe the deliberations of all public bodies or agencies of state government and its subdivisions, except in cases in which the demand of individual privacy clearly exceeds the merits of public disclosure.

Statutory Issues and Case Law

A. **Government records:**

2-6-101. Definitions. (1) Writings are of two kinds:

(a) public; and

(b) private.

(2) Public writings are:

(a) the written acts or records of the acts of the sovereign authority, of official bodies and tribunals, and of public officers, legislative, judicial, and executive, whether of this state, of the United States, of a sister state, or of a foreign country, except records that are constitutionally protected from disclosure;

(b) public records, kept in this state, of private writings, including electronic mail, except as provided in 22-1-1103 [library records] and 22-3-807 [burial site records] and except for records that are constitutionally protected from disclosure.

(3) Public writings are divided into four classes:

(a) laws;

(b) judicial records;

(c) other official documents;

(d) public records, kept in this state, of private writings, including electronic mail.

(4) All other writings are private.

B. Trade Secrets

Defined in 30-14-102(4): "Trade secret" means information or computer software, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(a) derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use; and

(b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Exempt from review as public writing under 2-6-102(3):

2-6-102. Citizens entitled to inspect and copy public writings. (1) Every citizen has a right to inspect and take a copy of any public writings of this state, except as provided in 22-1-1103, 22-3-807, or subsection (3) of this section and as otherwise expressly provided by statute.

(2) Every public officer having the custody of a public writing that a citizen has a right to inspect is bound to give the citizen on demand a certified copy of it, on payment of the legal fees for the copy, and the copy is admissible as evidence in like cases and with like effect as the original writing. The certified copy provision of this subsection does not apply to the public record of electronic mail provided in an electronic format.

(3) Records and materials that are constitutionally protected from disclosure are not subject to the provisions of this section. Information that is constitutionally protected from disclosure is information in which there is an individual privacy interest that clearly exceeds the merits of public disclosure, including legitimate trade secrets, as defined in 30-14-402, and matters related to individual or public safety.

(4) A public officer may withhold from public scrutiny information relating to individual privacy or individual or public safety or security of public facilities, including jails, correctional facilities, private correctional facilities, and prisons, if release of the information may jeopardize the safety of facility personnel, the public, or inmates of a facility. Security features that may be protected under this section include but are not limited to architectural floor plans, blueprints, designs, drawings, building materials, alarms system plans, surveillance techniques, and facility staffing plans, including staff numbers and locations. A public officer may not withhold from public scrutiny any more information than is required to protect an individual privacy interest or safety or security interest.

Court decisions cite Article II, Section 4 of the Montana Constitution:

> ***Individual dignity.*** *The dignity of the human being is inviolable. No person shall be denied the equal protection of the laws. Neither the state nor any person, firm,*

corporation, or institution shall discriminate against any person in the exercise of his civil or political rights on account of race, color, sex, culture, social origin or condition, or political or religious ideas.

Mtn. States Tel. & Tel. v. Dept. of Public Service Regulation, 194 M 277, 634 P2d 181, 38 St. Rep. 1479 (1981).

MCA Annotations under "Right to Know"

Economic Advantage Inadequate Reason for Denial of Public Right to Observe Government Deliberations in Corrections Vendor Process: *A newspaper company sought to restrain the Department of Corrections from excluding the public from meetings of the committee that reviewed proposals for operating private prison facilities. The District Court held that the public had no right to observe the negotiation phase of the committee's work, but that once negotiations were completed, the process by which the conclusions were arrived at must be open to public observation. Both parties appealed. The Supreme Court noted that as part of an Executive Branch agency, the Department and the committee were considered governmental bodies pursuant to 2-15-104 for purposes of procurement and that under the constitutional right to know, proposals submitted by private vendors were considered documents of a public body or agency that, under 2-6-102, the public has a right to inspect. Under the two-part test in Missoulian v. Bd. of Regents, 207 M 513, 675 P2d 962 (1984), the only exception to the constitutional provision arises when the demand of individual privacy clearly exceeds the merits of public disclosure. The state contended that the meetings at issue were closed for economic advantage, but economic advantage is neither a privacy interest nor a sufficient reason for denying the public the opportunity to observe deliberations of public bodies or to examine public documents, including proposals submitted to the public body by a vendor, unless the proposal concerns a privacy interest involving legitimate trade secrets or individual safety. A public agency's desire for privacy does not provide an exception to the public's constitutional right to observe its government at work. To the extent that provisions in 18-4-304 or ARM 2.5.602 require exclusion of the public from the competitive bid process, those provisions are unconstitutional and unenforceable.* Great Falls Tribune Co., Inc. v. Day, 1998 MT 133, 289 M 155, 959 P2d 508, 55 St. Rep. 524 (1998), following Mtn. States Tel. & Tel. Co. v. Dept. of Public Service Regulation, 194 M 277, 634 P2d 181 (1981), State ex rel. Great Falls Tribune Co., Inc. v. District Court, 238 M 310, 777 P2d 345 (1989), Great Falls Tribune Co., Inc. v. Great Falls Pub. Schools, 255 M 125, 841 P2d 502 (1992), and Common Cause of Mont. v. Statutory Comm. to Nominate Candidates for Comm'r of Political Practices, 263 M 324, 868 P2d 604 (1994).

Annotations under Title 69, Chapter 3, Part 1:

No Constitutional Right to Privacy for Nonhuman Entities -- Protection of Trade Secrets Under Other Constitutional and Statutory Schemes: Montana's constitutional individual privacy exception to the public's right to know is limited to natural human individuals only and does not apply to nonhuman entities such as corporations. However, nothing in Art. II, sec. 9, Mont. Const., requires disclosure of trade secrets and other confidential proprietary information when that data is protected from disclosure elsewhere in the state or federal constitution or by statute. Great Falls Tribune v. Mont. Pub. Serv. Comm'n, 2003 MT 359, 319 M 38, 82 P3d 876 (2003), overruling Mtn. States Tel. & Tel. v. Dept. of Public Service Regulation, 194 M 277, 634 P2d 181 (1981), and its progeny to the extent that those decisions relied on the constitutional balancing test of the right to individual privacy against the public's right to examine documents or observe governmental deliberations as a basis of protecting trade secrets and other confidential proprietary information of nonhuman entities.

Department of Justice -- confidentiality requirements:

in 23-5-115(6) -- The department may not make public or otherwise disclose confidential criminal justice information, as defined in 44-5-103, information obtained in the tax reporting processes, personal information protected by an individual privacy interest, or trade secrets, as defined in 30-14-402, specifically identified and for which there are reasonable grounds of privilege asserted by the party claiming the privilege.

in 23-5-116-- Disclosure of information. (1) The department shall, upon request, disclose information concerning a current or former gambling license applicant or gambling licensee or any other person engaged in gambling or a gambling activity governed by parts 1 through 8 of this chapter, except:

(a) confidential criminal justice information, as defined in 44-5-103;

(b) personal information protected by an individual privacy interest;

(c) trade secrets, as defined in 30-14-402, specifically identified and for which there are reasonable grounds of privilege asserted by the party claiming the privilege; and

(d) information obtained in the tax reporting processes.

(2) Notwithstanding the limitations set forth in subsection (1), the department may disclose any information obtained in the application or tax reporting process or as a result of other department operations to:

(a) a federal, state, city, county, or tribal criminal justice agency;

(b) the department of revenue and the federal internal revenue service; and

(c) a gambling regulatory agency of another state, a local government unit of another state, a tribal government, or a foreign nation, provided that the disclosure of the information complies with the law of that jurisdiction and that the receiving entity has been approved for receipt by the Montana attorney general.

(3) In the event of a tax delinquency or at the request of a video gambling machine permitholder, the department shall inform the permitholder of the status of a licensed machine owner's tax payments for a video gambling machine located at the permitholder's place of business.

44-5-103 (3) "Confidential criminal justice information" means:

(a) criminal investigative information;

(b) criminal intelligence information;

(c) fingerprints and photographs;

(d) criminal justice information or records made confidential by law; and

(e) any other criminal justice information not clearly defined as public criminal justice information.

State Auditor/Insurance Department -- confidentiality:

of examiner's report in 33-1-409 (4 through 6 specifically)

(4) (a) All orders entered pursuant to subsection (3)(a) must be accompanied by findings and conclusions resulting from the commissioner's consideration and review of the examination report, relevant examiner workpapers, and any written submissions or rebuttals. An order must be considered a

final administrative decision and may be appealed pursuant to Title 33, chapter 1, part 7, and must be served upon the company by certified mail, together with a copy of the adopted examination report. Within 30 days of the issuance of the adopted report, the company shall file affidavits executed by each of its directors stating under oath that they have received a copy of the adopted report and related orders.

(b) (i) A hearing conducted under subsection (3)(c) by the commissioner or an authorized representative must be conducted as a nonadversarial, confidential, investigatory proceeding as necessary for the resolution of any inconsistencies, discrepancies, or disputed issues apparent upon the face of the filed examination report or raised by or as a result of the commissioner's review of relevant workpapers or by the written submission or rebuttal of the company. Within 20 days of the conclusion of the hearing, the commissioner shall enter an order pursuant to subsection (3)(a).

(ii) The commissioner may not appoint an examiner as an authorized representative to conduct the hearing. The hearing must proceed expeditiously with discovery by the company limited to the examiner's workpapers that tend to substantiate any assertions set forth in any written submission or rebuttal. The commissioner or the commissioner's representative may issue subpoenas for the attendance of witnesses or the production of documents considered relevant to the investigation, whether under the control of the department, the company, or other persons. The documents produced must be included in the record, and testimony taken by the commissioner or the commissioner's representative must be under oath and preserved for the record. This section does not require the department to disclose any information or records that would indicate or show the existence or content of an investigation or activity of a criminal justice agency.

(iii) The hearing must proceed with the commissioner or the commissioner's representative posing questions to the persons subpoenaed. The company and the department may present testimony relevant to the investigation. Cross-examination may be conducted only by the commissioner or the commissioner's representative. The company and the department must be permitted to make closing statements and may be represented by counsel of their choice.

(5) (a) Upon the adoption of the examination report under subsection (3)(a), the commissioner shall continue to hold the content of the examination report as private and confidential information for a period of 30 days, except to the extent provided in subsection (2). After 30 days, the commissioner shall open the report for public inspection as long as a court of competent jurisdiction has not stayed its publication.

(b) This title does not prevent and may not be construed as prohibiting the commissioner from disclosing the content of an examination report or preliminary examination report, the results of an examination, or any matter relating to a report or results to the insurance department of this state or of any other state or country, to law enforcement officials of this state or of any other state, or to an agency of the federal government at any time as long as the agency or office receiving the report or matters relating to the report agrees in writing to hold it in a manner consistent with this part.

(c) If the commissioner determines that regulatory action is appropriate as a result of an examination, the commissioner may initiate any proceedings or actions as provided by law.

(6) All working papers, confidential criminal justice information, as defined in 44-5-103, personal information protected by an individual privacy interest, and trade secrets, as defined in 30-14-402, specifically identified and for which there are reasonable grounds of privilege asserted by the party claiming the privilege obtained by or disclosed to the commissioner or any other person in the course of an examination made under this part must be given confidential treatment, are not subject to subpoena, and may not be made public by the commissioner or any other person, except to the extent provided in subsection (5). Access may also be granted to the NAIC. The persons given access to confidential criminal justice information, trade secrets, and personal information shall agree in writing,

prior to receiving the information, to treat the information in the manner required by this section unless the prior written consent of the company to which it pertains has been obtained.

General insurance confidentiality:

33-2-1116. Confidentiality of information. All confidential criminal justice information, as defined in 44-5-103, personal information protected by an individual privacy interest, and trade secrets, as defined in 30-14-402, specifically identified and for which there are reasonable grounds of privilege asserted by the party claiming the privilege obtained by or disclosed to the commissioner or any other person in the course of an examination or investigation made pursuant to 33-2-1115 and all information reported pursuant to 33-2-1111 and 33-2-1112 containing confidential criminal justice information, trade secrets, or personal information must be given confidential treatment, may not be subject to subpoena, and may not be made public by the commissioner or any other person, except to insurance departments of other states, without the prior written consent of the insurer to which it pertains unless the commissioner, after giving the insurer and its affiliates who would be affected notice and opportunity to be heard, determines that the interests of policyholders, shareholders, or the public will be served by the publication of the trade secrets or personal information, in which event the commissioner may publish all or any part of the trade secrets or personal information in a manner that the commissioner considers appropriate.

Requirements for Insurance Administrators:

33-17-611. Maintenance of information. For the duration of the agreement required by 33-17-602 and for 5 years thereafter, each administrator shall maintain at its principal administrative office adequate books and records of all transactions between the administrator, insurers, and insured persons. These books and records must be maintained in accordance with prudent standards of insurance recordkeeping. The commissioner shall have access to these books and records for examination, audit, or inspection. Any trade secrets contained in the books and records, including but not limited to the identity and addresses of policyholders and certificate holders, are confidential, except that the commissioner may use the information in any proceedings instituted against the administrator. The insurer retains the right to continuing access to those books and records of the administrator sufficient to permit the insurer to fulfill all of its contractual obligations to insured persons, subject to any restrictions in the written agreement between the insurer and the administrator.

Requirements for Health Maintenance Organizations:

33-31-112. Filings and reports as public documents. All applications, filings, and reports required under this chapter, except those that contain trade secrets or privileged or confidential commercial or financial information (other than an annual financial statement that the commissioner may require under 33-31-211), are public documents.

Requirements for the Interstate Commission for Juveniles (under Article III of the interstate compact), which is similar to Article II, activities for the Commission regarding the interstate compact for adult offender supervision):

(9) Public notice must be given of all meetings, and all meetings must be open to the public except as set forth in the rules or as otherwise provided in the compact. The interstate commission and any of its committees may close a meeting to the public when it determines by two-thirds vote that an

open meeting would be likely to:

(a) relate solely to the interstate commission's internal personnel practices and procedures;

(b) disclose matters specifically exempted from disclosure by statute;

(c) disclose trade secrets or commercial or financial information that is privileged or confidential;

(d) involve accusing any person of a crime or formally censuring any person;

(e) disclose information of a personal nature when disclosure would constitute a clearly unwarranted invasion of personal privacy;

(f) disclose investigative records compiled for law enforcement purposes;

(g) disclose information contained in or related to examination, operating, or condition reports prepared by, or on behalf of or for the use of, the interstate commission with respect to a regulated person or entity for the purpose of regulation or supervision of the person or entity;

(h) disclose information, the premature disclosure of which would significantly endanger the stability of a regulated person or entity; and

(i) specifically relate to the interstate commission's issuance of a subpoena or its participation in a civil action or other legal proceeding.

Public Service Commission requirements:

69-3-105. Access to commission records and reports -- protective order. (1) Except as provided in subsection (2), the reports, records, accounts, files, papers, and memoranda of every nature in the possession of the commission are open to the public during regular business hours, as defined in 2-16-117.

(2) The commission may issue a protective order when necessary to preserve trade secrets, as defined in 30-14-402, or other information that must be protected under law, as required to carry out its regulatory functions.

Dept. of Environmental Quality requirements:

75-5-105. Confidentiality of records. Except as provided in 80-15-108, any information concerning sources of pollution which is furnished to the board or department or which is obtained by either of them is a matter of public record and open to public use. However, any information unique to the owner or operator of a source of pollution which would, if disclosed, reveal methods or processes entitled to protection as trade secrets shall be maintained as confidential if so determined by a court of competent jurisdiction. The owner or operator shall file a declaratory judgment action to establish the existence of a trade secret if he wishes such information to enjoy confidential status. The department shall be served in any such action and may intervene as a party therein. Any information not intended to be public when submitted to the board or department shall be submitted in writing and clearly marked as confidential. The data describing physical and chemical characteristics of a waste discharged to state waters shall not be considered confidential. The board may use any information in compiling or publishing analyses or summaries relating to water pollution if such analyses or summaries do not identify any owner or operator of a source of pollution or reveal any information which is otherwise made confidential by this section.

75-10-707. Information gathering and access. (1) The department may undertake any

investigative or other information-gathering action that it considers necessary or appropriate for determining the need for remedial action, choosing or taking a remedial action, or otherwise enforcing the provisions of this part. ...

(8) Persons subject to the requirements of this section may make a written claim of confidentiality for information unique to the owner or operator of a facility that would, if disclosed, reveal methods or processes entitled to protection as trade secrets. The claim of confidentiality must be clearly designated on the materials at the time they are obtained by the department. If the department accepts the characterization, it shall maintain that information as confidential. Information describing physical or chemical characteristics of hazardous or deleterious substances that have been or may be released into the environment are not considered confidential. The department has access to and may use any trade secret information in carrying out the activities of this part as may be necessary to protect the public health, safety, or welfare or the environment while maintaining the information as confidential.

Board of Oil and Gas Conservation requirements:

82-11-117. Confidentiality of records. (1) Any information that is furnished to the board or the board's staff or that is obtained by either of them is a matter of public record and open to public use. However, any information unique to the owner or operator that would, if disclosed, reveal methods or processes entitled to protection as trade secrets must be maintained as confidential if so determined by the board.

(2) If an owner or operator disagrees with a determination by the board that certain material will not be maintained as confidential, the owner or operator may file a declaratory judgment action in a court of competent jurisdiction to establish the existence of a trade secret if he wishes such information to enjoy confidential status. The department must be served in any such action and may intervene as a party.

(3) Any information not intended to be public when submitted to the board or the board's staff must be submitted in writing and clearly marked as confidential.

(4) Data describing physical and chemical characteristics of a liquid, gaseous, solid, or other substance injected or discharged into state waters may not be considered confidential.

(5) The board may use any information in compiling or publishing analyses or summaries relating to water pollution if such analyses or summaries do not identify the owner or operator or reveal any information that is otherwise made confidential by this section.

Energy information available to governor under emergency situations, and disclosure constraints:

90-4-305. Information obtainable by governor. (1) The governor may obtain information on a regular basis from energy resource producers, suppliers, public agencies, and consumers and from political subdivisions in this state that is necessary for the governor to determine the need for energy supply alert and emergency declarations. The information may include but is not limited to: ...

(2) In order to help anticipate and mitigate the effects of shortages of petroleum products, the governor may monitor the supply of and demand for these products by obtaining the following monthly reports submitted no later than 20 days after the last day of the month, on forms prescribed by the governor, from the following persons:....

(5) Except as provided in subsection (2), this part does not require the disclosure by a distributor of confidential information, trade secrets, or other facts of a proprietary nature.

II. Data Storage and Disposal

General

2-6-213. Agency responsibilities and transfer schedules. Each executive branch agency of state government shall administer its records management function and shall:

(1) coordinate all aspects of the agency records management function;

(2) manage the inventorying of all public records within the agency for disposition, scheduling, and transfer action in accordance with procedures prescribed by the secretary of state and the state records committee;

(3) analyze records inventory data, examine and compare divisional or unit inventories for duplication of records, and recommend to the secretary of state and the state records committee minimal retentions for all copies of public records within the agency;

(4) approve all records disposal requests that are submitted by the agency to the state records committee;

(5) review established records retention schedules to ensure that they are complete and current; and

(6) officially designate an agency records custodian to manage the functions provided for in this section.

Judiciary statutory references:

3-1-114. Definitions. As used in 3-1-115 and this section, the following definitions apply:

(1) "Document" means all contents in the file or record of any case or matter docketed by a court, including decisions, administrative orders, court records, court books, court minutes and minute books, court dockets, court ledgers, registers of actions, court indexes, and other documents, instruments, or papers required by law to be filed with a court.

(2) "Electronic filing of documents" means the transmission of data to a court by the communication of information that is originally displayed in written form and then converted to digital electronic signals, transformed by computer, and stored by the clerk of the court on microfilm, magnetic tape, optical disc, or other medium.

(3) "Electronic storage of documents" means the recording, storage, retention, maintenance, and reproduction of court documents, using microfilm, microfiche, data processing, computers, or other electronic processes that correctly and legibly store and reproduce documents.

3-1-115. Electronic filing and storage of documents -- rules. (1) The supreme court may make rules establishing procedures for electronic filing of documents and electronic storage of documents.

(2) Courts may, but are not required to, institute procedures for electronic filing of documents and electronic storage of documents to further the efficient administration and operation of the courts. Electronically filed or stored documents may be kept in lieu of any paper documents. Electronic filing of documents and electronic storage of documents must be in conformity with rules adopted by the supreme court.

(3) The provisions of 3-1-114 and this section may not be construed to repeal any other provision of existing law that requires or provides for the maintenance of official written documents, records, dockets, books, ledgers, or proceedings by a court or clerk of the court in those courts that do not institute electronic filing of documents and electronic storage of documents.

(4) The procedures for electronic storage of documents may require but are not limited to the following:

(a) all original documents to be recorded and released into the court's electronic filing and storage system within a specified minimum time period after presentation to the court;

(b) the use of original paper records during the pendency of any legal proceeding;

(c) standards for organizing, identifying, coding, indexing, and reproducing an original document so that an image produced from electronically stored information can be certified as a true and correct copy of the original and can be retrieved rapidly; and

(d) retention of the original documents consistent with other law and security provisions to guard against physical loss, alterations, and deterioration.

HB 732 Requirement

30-14-1703. (Effective March 1, 2006) Record destruction. A business shall take all reasonable steps to destroy or arrange for the destruction of a customer's records within its custody or control containing personal information that is no longer necessary to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable.

Financial

32-1-492. Definitions -- reproduction of bank records -- admissibility in evidence -- cost recovery. (1) (a) For the purposes of this section, "bank records" includes any document, paper, letter, book, map, photograph, sound or video recording, magnetic tape, electronic-storage medium, or other information- recording medium used in a bank's normal course of business.

(b) (i) For the purposes of this section, "electronic storage" means the recording, storage, retention, maintenance, and reproduction of documents using microfilm, microfiche, data processing, computers, or other electronic process that correctly and legibly stores and reproduces documents.

(ii) A photographic, photostatic, miniature photographic copy, or reproduction of any kind, including electronic or computer-generated data that has been electronically stored and is capable of being converted into written form, must be considered an original record for all purposes and must be treated as an original record in all courts and administrative agencies for the purposes of admissibility in evidence.

(iii) A facsimile, exemplification, or certified copy of any reproduction referred to in subsection (1)(b)(ii) must, for all purposes, be considered a facsimile, exemplification, or certified copy of the original record.

(2) Except as provided in subsection (6), banks are authorized to make, at any time, photographic or photostatic copies or microfilm reproductions of any records or documents, including photographic enlargements and prints of microfilms, to be preserved, stored, used, and employed in carrying on business.

(3) In an action or proceeding in which bank records may be called in question or be demanded of a bank or any officer or employee of a bank, a showing that the records have been destroyed in the regular course of business is a sufficient excuse for the failure to produce the records.

(4) Upon the showing required in subsection (3), secondary evidence of the form, text, and contents of the original records, including photostatic, photographic, or microfilm reproductions,

photographic enlargements, and prints of microfilm reproductions, when made in the regular course of business, is admissible in evidence in any court of competent jurisdiction or in any administrative proceeding.

(5) Any photostatic, photographic, or microfilm reproductions, including enlargements of the microfilm reproductions, made in the regular course of business of any original files, records, books, cards, tickets, deposit slips, or memoranda that were in existence on July 1, 1951, are admissible in evidence as proof of the form, text, and content of the originals that were destroyed in the regular course of business.

(6) A bank may, as a condition of providing bank records to a third party in response to a subpoena or to another legal procedure or request, charge and collect the actual costs incurred in locating, reproducing, and providing the bank records.

Criminal Justice Data

44-5-403. Computer programming. Procedures for each automated criminal justice information system shall assure that the information is secured by the following programming techniques and security procedures:

(1) the assignment of a terminal identification code to each terminal authorized to access the criminal justice information system;

(2) the assignment of a unique identification number to each authorized terminal operator, which number must be used to gain access to the files;

(3) the maintenance of a record of each inquiry to identify the inquiring agency, the program used to make the inquiry, the date of the inquiry, and the name of the file being queried;

(4) computer programming controls to ensure that each terminal user can obtain only that information which the user is authorized to use;

(5) creation and use of a safe place for storage of duplicate computer files;

(6) built-in program controls to ensure that each terminal is limited to the appropriate or authorized information that can be input, modified, or canceled from it;

(7) destruction or safeguarding of system documentation and data input forms; and

(8) creation of reports to provide for an audit trail and periodic review of file accessed, modifications, and deletions. All criminal justice intelligence information shall be identified as such.

National Crime Prevention and Privacy Compact

The purposes of this compact are to:

(1) provide a legal framework for the establishment of a cooperative federal-state system for the interstate and federal-state exchange of criminal history records for noncriminal justice uses;

(2) require the FBI to permit use of the national identification index and the national fingerprint file by each party state and to provide, in a timely fashion, federal and state criminal history records to requesting states, in accordance with the terms of this compact and with rules, procedures, and standards established by the council under Article VI;

(3) require party states to provide information and records for the national identification index and the national fingerprint file and to provide criminal history records, in a timely fashion, to criminal history record repositories of other states and the federal government for noncriminal justice purposes, in

accordance with the terms of this compact and with rules, procedures, and standards established by the council under Article VI;

(4) provide for the establishment of a council to monitor III system operations and to prescribe system rules and procedures for the effective and proper operation of the III system for noncriminal justice purposes; and

(5) require the FBI and each party state to adhere to III system standards concerning record dissemination and use, response times, system security, data quality, and other duly established standards, including those that enhance the accuracy and privacy of such records.

Question:

Do state and local government agencies as well as businesses need more "direction" for storing or disposing of personally identifiable data?

S1332 introduced by Senators Leahy and Specter requires various data security measures for business entities engaging in interstate commerce, based on the Office of the Comptroller of the Currency guidelines for financial institutions. That particular bill does not preempt state laws that provide more consumer protection. Other bills in Congress do provide preemption. Does the work group want to make a recommendation?

III. Background Information on TPMs (Third-party Marketers)

According to the website www.americanbrokerage.com, third-party marketing grew from 2 firms in 1982 to more than 300 firms providing investment products and services to banking institutions in 1994. Since then, consolidation has taken place. Today about 100 TPMs exist.

S1332 also addresses data brokerage and seeks to fill in the gaps under FCRA and Gramm-Leach-Bliley. S1332 wold apply to a business entity that "for monetary fees, dues, or on a cooperative basis, regularly engages, in whole or in part, in the practice of collecting, transmitting, or otherwise providing personally identifiable information on a nationwide basis on more than 5,000 individuals who are not the customers or employees of the business entity or affiliate."

Legislation affecting third-party marketers includes:

1. California's "Shine the Light" Law -- I will provide a copy along with Montana's proposed, but not enacted, version from HB 732.

2. parts of HIPAA -- 45 CFR 164.501 and 508(a)(3)

3. parts of FCRA

4. GLB provides "opt-out", generally allows contacts with own customers, requires disclosure - See FTC website: http://www.ftc.gov/privacy/glbact/glbsub1.htm#6801.