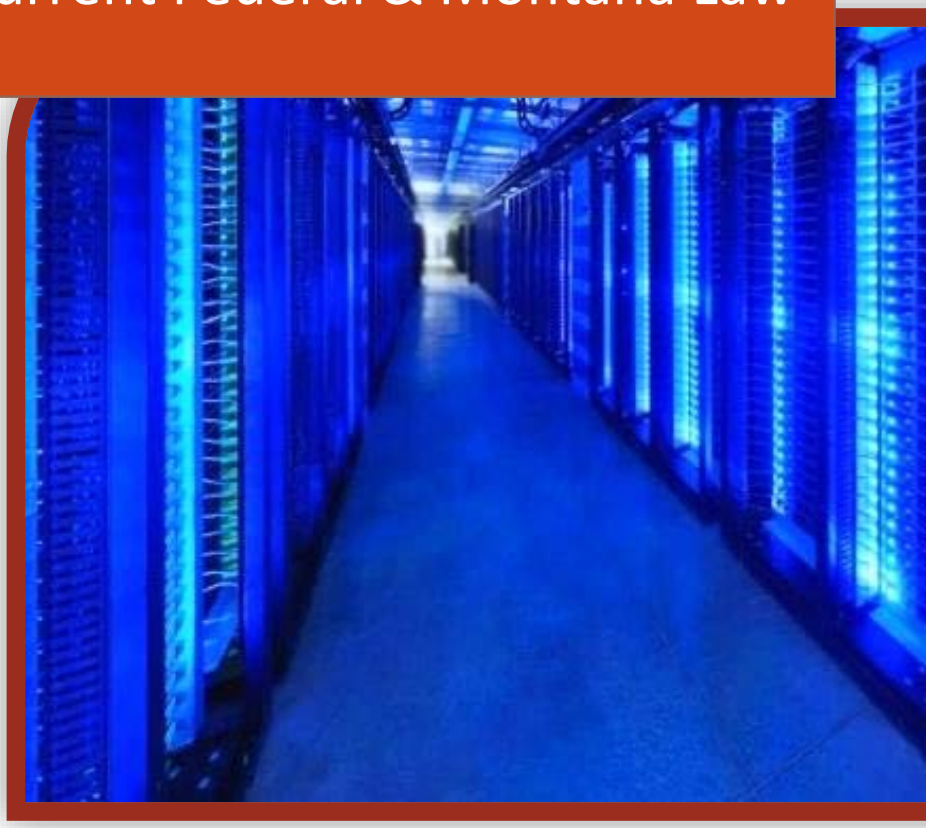
HJR 21 Study of Personal Information Ownership:
Overview of Current Federal & Montana Law



This paper is an unedited presentation outline.

For the

State Administration and Veterans' Affairs Interim Committee

By Sheri S. Scurr, Research Analyst
Montana Legislative Services
November 2015
sscurr@mt.gov

Executive Summary

Personal Information Ecosystem

An entire ecosystem surrounds the collection, storage, sale, and use of individual and aggregated personal information. A diagram showing all of the various people and entities that have a stake in the ownership and control of personal information shows the individual at the center of system surrounded by wider concentric circles. Each circle consists of various players. The diagram helps with understanding the big picture that is often described as the world of "big data". The circles of stakeholders within the diagram that surround the individual are described below (the diagram itself is too complex to reasonably fit on this 8 ½ x 11 page) :

- Smallest Circle – Data Collectors:
    - Internet sites – such as:
        - Search engines
        - Social networks
        - Online shopping
    - Medical entities- such as:
        - Hospitals
        - Doctors
        - Pharmacies
    - Financial entities – such as:
        - Banks
        - Insurance companies
        - Stock brokers
    - Telecommunication & mobile service providers
        - Cell phone companies
        - Cable companies
        - Internet and Wi-Fi carriers
    - Retail companies – such as:
        - Airlines
        - Credit card companies
        - Stores
    - Public – such as:
        - Media
        - Government
        - Utilities
- Middle Circle - Data Brokers
    - Marketing companies
    - Website analytic companies
    - Media companies
    - Credit Bureaus
    - Healthcare analytics companies
    - Advertiser networks
    - Catalogue co-ops

    - List brokers
    - Affiliates
- Widest Circle – Data Users
    - Advertisers
    - Media companies
    - Government agencies
    - Attorneys and private investigators
    - Individuals
    - Law enforcement agencies
    - Product and service providers
    - Employers
    - Financial institutions

Legal Environment

The personal information ecosystem exists within a framework or current laws. Current federal law related to personal information has been characterized as a patchwork of overlapping and sometimes inconsistent laws involving several different government agencies and complex implementing regulations. Additionally, many federal regulations are really just "best practice" guidelines that encourage self-regulation and rely on voluntary compliance.[1]

State laws concerning how personal data is handled also vary widely. In general, federal law governs when state laws are less restrictive. However, there are still gray areas where it is unclear whether state or federal laws would govern. Still, several states have enacted more restrictive laws and laws that fill gaps in the fabric of the federal laws. [2]

Entities that collect, use, secure, or distribute personal information must comply with both federal and state laws. [3]

Most of federal and state laws seem aimed at particular industries, business types, or agencies, such as online retailers, financial institutions, public agencies, or health care providers. Some laws cover only specific types of information, such as health information, information about a specific demographic population, such as minors, or information related to a specific use, such as for research or homeland security.

[1] Iuean Jolly, "Data Protection in the United States: Overview," Practical Law Company by Thomson Reuters, July 1, 2014, available at http://us.practicallaw.com/6-502-0467.

[2] Ibid.

[3] Jolly, "Data Protection in the United States: Overview."

Scope of Report

This report provides only a general overview of some of the main federal and state laws governing certain types of personal information:

- consumer data;
- financial; and
- health.

Each of these data categories is discussed in the context of:

- covered information;
- covered entities;
- individual rights;
- oversight and enforcement.

Federal Laws

The federal laws included in this report are the following:

- Federal Trade Commission Act (15 U.S.C. Subchapter I);
- Personal Data Protection and Breach Accountability Act of 2014 (S. 1995, 113th Congress);
- Financial Services Modernization Act (Gramm-Leach-Baily Act (GLB)) (15 U.S.C. 6801 through 6827);
- Fair Credit Reporting Act (15 U.S.C. 1681); and
- Health Insurance Portability and Accountability Act (Public Law 104-191, 1996).[4]

Montana Laws

Montana Code Annotated (MCA) provisions covered in this report include the following:

- the Montana Unfair Trade Practices and Consumer Protection Act (Title. 30, ch. 14, part 1, MCA)
- a prohibition against unfair or deceptive trade practices by insurers (section 33-18-102, MCA);
- the Insurance Information and Privacy Protection Act (Title 33, ch. 19, MCA);

[4] This is not an exhaustive list of federal laws that may be applicable to the collection and use of personal information.

- impediment to identify theft provisions (Title 30, ch. 14, part 1, MCA);
- state agency protection of personal information provisions (Title 2, ch. 6, part 15, MCA);
- the Montana Information Technology Act (Title 2, ch. 17, part 5, MCA);
- health care information provisions (Title 50, ch. 16, MCA).[5]
    - Uniform Health Care Information Act – Part 5
    - Government Health Care Information Act – Part 6
    - Health Care Information Privacy Requirements for Providers Subject to HIPAA – Part 8

Policy Topics

There are a wide range of policy topics within the scope of a study on personal information. NCSL has most recently written about the following topics:

- access to social media user names and passwords;
- security breach notification;
- ownership of the "digital assets" of a decedent;
- facial recognition technology and biometric data;
- automated license plate readers;
- online reputation protection companies;
- computer crime and phishing scams;
- the personal data of students;
- "smart meter" technology available to electric utility companies;
- disposal/retention of personal data;
- access to law enforcement information such as 911 calls and body camera recordings;
- event data recording technology (e.g., a "black box" in a vehicle);
- online privacy protection, especially for minors, such as "do not track" options;
- employer monitoring of e-mail or internet use;
- Radio Frequency Identification technology;
- e-reader privacy in libraries; and
- promoting careers in the cyber security industry.

Ownership of Personal Information

With respect to the policy question about who owns what personal information, "ownership" of personal information has been discussed by scholars in various ways, such as:

[5] This is not an exhaustive list of state laws that may be applicable to the collection and use of personal information.

- a bundle of rights similar to the rights of land owners;[6]
- similar to ownership of intellectual property;[7]
- a commodity in the market place of personal information;[8]
- a right to define one's own identity;[9] and
- a right to control what personal information is collected, shared, and used.[10]

Many of these discussions contrast "ownership" with "privacy". However, they also acknowledge the legal and practical shortcomings of ownership theories and acknowledge that privacy rights themselves fall into two categories – the right to keep personal information secret and the right to control the information.[11] Thus, the policymaking waters surrounding the question of who owns what information are muddy and the distinction between personal information ownership and privacy is still unclear.

Federal Agencies

Overview

The main federal agencies with a key role in the oversight and control of personal information are the:

- Federal Trade Commission;
- Federal Communications Commission;
- Department of Public Health and Human Services;
- Department of Justice;

---

[6] Jane B. Baron, *Property as Control: The Case of Information*, 18 Mich. Telecomm. Tech L. Rev. 367 (2012). Available at http://www.mttlr.org/voleighteen/baron.pdf.

[7] See Pamela Samuelson, *Privacy as Intellectual Property*, Faculty Paper, Information Management and Law Professor, University of California at Berkeley. See also Dorothy J. Glancy, *Personal Information as Intellectual Property*, Faculty Abstract, Professor at Santa Clara University School of Law.

[8] Paul M. Schwartz, *Property, Privacy, and Personal Data,* 117 Harvard Law Review 2056 (2003-2004). Downloaded from HeinOnline (http://heinonline.org).

[9] Baron, *Property as Control: The Case of Information*.

[10] Schwartz, *Property, Privacy, and Personal Data*.

[11] Vera Bergelson, *It's Personal but Is It Mine? Toward Property Rights in Personal Information,* Rutgers University (Newark) Legal Working Paper Series, 2003, p. 401. Available at: http://works.bepress.com/vera_bergelson/2.

- Department of Homeland Security; and
- Department of Commerce.

Federal Trade Commission

The Federal Trade Commission was established in 1914. It is a 5-member commission appointed by the U.S. President with the advice and consent of the U.S. Senate. The mission of the FTC is to protect consumers and promote and protect fair competition.[12] To fulfill this mission, the FTC is empowered to:

- prosecute unfair, deceptive, or fraudulent business practices;
- seek monetary redress and other relief for business conduct that harms consumers;
- prescribe trade regulation rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices;
- conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce; and
- make reports and legislative recommendations to Congress.[13]

With respect to personal data, the Federal Trade Commission Act authorizes the Commission to file court actions against any company doing business in the United States that:

- fails to protect personal data;
- changes its privacy policy without adequate notice; or
- fails to comply with its posted privacy policy.[14]

Federal Communications Commission

The Federal Communications Commission was established in 1934. Its five members are appointed by the President with the advice and consent of the U.S. Senate. The FCC regulates interstate and international communications by radio, television, wire, satellite and cable in all 50 states, the District of Columbia and U.S. territories. The agency's website states that its mission is to:

- promote competition, innovation and investment in broadband services and facilities;
- support the nation's economy by ensuring an appropriate competitive framework for the unfolding of the communications revolution;
- encourage the highest and best use of spectrum domestically and internationally;

---

[12] Federal Trade Commission webpage at https://www.ftc.gov/about-ftc/our-history.

[13] Federal Trade Commission webpage at https://www.ftc.gov/enforcement/statutes.

[14] Federal Trade Commission Act, 15 U.S.C. 41-58, available at https://www.ftc.gov/enforcement/statutes/federal-trade-commission-act.

- revise media regulations so that new technologies flourish alongside diversity and localism; and
- provide leadership in strengthening the defense of the nation's communications infrastructure.[15]

U.S. Department of Health and Human Services

The Department of Health and Human Services (HHS) is required under the Health Insurance Portability and Accountability Act of 1996 (HIPPA) to publish standards for the exchange, privacy, and security of certain personal health. The standards, known as the Privacy Rule is a covers the use and disclosure of "protected health information" by "covered entities." The Privacy Rule also sets standards concerning the rights individuals have to be informed and to control how their health information is used. The Office for Civil Rights within the HHS is responsible for implementing the Privacy Rule.

U.S. Department of Justice/ U.S. Department of Homeland Security

The U.S. Department of Justice partners with the U.S. Department of Homeland Security to provide resources and training to law enforcement agencies concerning the protection of privacy and civil liberties. The agencies have developed a "one-stop-shop" web portal. The portal provides access to a training tool kit, various guides and templates, and other resources related to privacy and civil rights. The departments develop standards, guidelines, and policies with respect to the electronic collection of personal information, including biometric data through the use of facial recognition, finger print scanning, or iris scanning technologies.[16]

U.S. Department of Commerce

The National Telecommunications and Information Administration

Within the Department of Commerce is an organization called the National Telecommunications and Information Administration (NTIA). Part of the NTIA's mission is advising the President on telecommunications and information policy issues concerning use of the Internet and "ensuring the Internet remains an engine for continued innovation and economic growth".[17] The department established an Internet Policy Task Force "to conduct a comprehensive review of the nexus between privacy policy, copyright, global free flow of information, cybersecurity, and innovation in the Internet economy."[18] Initiatives of the task force encompass privacy and cyber security.

Consumer Privacy Bill of Rights

In December 2010, the NTIA's Internet Policy Task Force released a discussion draft of proposed legislation called the Consumer Privacy Bill of Rights. This document reflects the following policy principles as articulated by the task force report:

[15] Federal Communications Commission web page at https://www.fcc.gov/what-we-do.
[16] See web portal at http://www.it.ojp.gov/PrivacyLiberty.
[17] NTIA mission statement at http://www.ntia.doc.gov/.
[18] Internet Policy Task Force web page at http://www.ntia.doc.gov/category/internet-policy-task-force.

- **Individual Rights:** Consumers have a right to exercise control over what personal data companies collect from them and how they use it.

- **Transparency:** Consumers have a right to easily understandable and accessible information about privacy and security practices.

- **Respect for Context:** Consumers have a right to expect that companies will collect, use, and disclose personal data in ways that are consistent with the context in which consumers provide the data.

- **Security:** Consumers have a right to secure and responsible handling of personal data.

- **Access and Accuracy:** Consumers have a right to access and correct personal data in usable formats, in a manner that is appropriate to the sensitivity of the data and the risk of adverse consequences to consumers if the data is inaccurate.

- **Focused Collection:** Consumers have a right to reasonable limits on the personal data that companies collect and retain.

- **Accountability:** Consumers have a right to have personal data handled by companies with appropriate measures in place to assure they adhere to the Consumer Privacy Bill of Rights.

Federal Laws

Federal Trade Commission Act - 15 U.S.C. 41-58

Overview

The Federal Trade Commission Act prohibits unfair methods of competition and unfair or deceptive acts or practices in or affecting commerce.

Covered Information

The FTC Act does not apply to any specific type of personal information. Instead, it prohibits any unfair or deceptive practices related to consumers' personal information, such as:

- failure to protect consumer personal data;
- not providing adequate notice about a change to a company's privacy policy; or
- failure to comply with a posted privacy policy.

The FTC Act does not require a company to have or disclose a privacy policy.[19]

Covered Entities

The FTC Act applies to most companies and individuals doing business in the U.S.. However, it does not apply to certain transportation, telecommunications, or financial companies because these industries are primarily regulated by other federal agencies and laws.[20]

Individual Rights

The FTC Act does not articulate specific consumer rights to control their personal information. However, because the Act prohibits "deceptive" practices, the FTC's position is that if a company has a personal information policy, the user has the right to:

- know what the policy is;
- be notified of any changes to the policy; and
- opt out if there have been changes to the policy.[21]

Oversight and Enforcement

Under the FTC Act, the FTC is authorized to:

- initiate civil prosecution for unfair and deceptive business practices;
- seek monetary redress and other relief for conduct injurious to consumers;
- prescribe trade regulation rules defining with specificity acts or practices that are unfair or deceptive, and establishing requirements designed to prevent such acts or practices;
- conduct investigations relating to the organization, business, practices, and management of entities engaged in commerce;
- make reports and legislative recommendations to Congress; and
- educate consumers and businesses.

Personal Data Protection and Breach Accountability Act of 2014 (S.1995 — 113th Congress)

Covered Personal Information

The Personal Data Protection and Breach Accountability Act of 2014 covers "sensitive personally identifiable information," which is substantially defined as follows:

---

[19] Ieuan Jolly, "Data protection in the United States: Overview," *Practical Law,* Thomson Reuters, July 2014.

[20] Ibid.

[21] Ieuan Jolly, "Data protection in the United States: Overview," *Practical Law,* Thomson Reuters, July 2014.

- An individual's first and last name or first initial and last name in combination with any 2 of the following data elements:
    - Home address.
    - Telephone number.
    - Mother's maiden name.
    - Month, day, and year of birth.

- A non-truncated social security number, driver's license number, passport number, or alien registration number or other government-issued unique identification number.

- Geographic location derived from a wireless communication device or other electronic device.

- Unique biometric data such as a fingerprint, voice print, face print, a retina or iris image, or any other unique physical representation.

- A unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, health insurance policy or subscriber identification number, or routing code.

- Not less than 2 of the following data elements:
    - first and last name or first initial and last name.
    - unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.
    - any security code, access code, or password, or source code that could be used to generate such codes and passwords.
    - information regarding an individual's medical history, mental or physical medical condition, or medical treatment or diagnosis by a health care professional.

- Any other combination of data elements that could allow unauthorized access to or acquisition of the information described above including:
    - a unique account identifier;
    - an electronic identification number;
    - a user name;
    - a routing code; or
    - any associated security code, access code, or password or any associated security questions and answers that could allow unauthorized access to the account.

Covered Entities

- Certain provisions apply to web service providers.
- Other provisions apply to any interstate business entity that collects, accesses, transmits, uses, stores, or disposes of sensitive personally identifiable information (PII) on 10,000 or more U.S. persons.

- The Act exempts certain public records, certain financial institutions subject to the Gramm-Leach-Bliley Act, business entities subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and service providers exclusively engaged in the transmission, routing, or storage of data.

Individual Rights

- Internet user must consent before a covered entity redirects, monitors, manipulates, aggregates, or markets sensitive PII data obtained from a website.

- Requires notification of individuals if there is a data security breach and provision of free quarterly consumer credit reports for 2-years and credit monitoring, a security freeze on the individual's credit report, and compensation for damages incurred.

Oversight and Enforcement

- Amends the federal criminal code to impose a fine and/or prison term of up to five years for intentionally or willfully concealing a security breach involving sensitive personally identifiable information when such breach results in economic harm or substantial emotional distress to one or more persons.

- Authorizes the U.S. Attorney General and State Attorneys General to bring civil actions for willful violations.

Financial Services Modernization Act (Gramm-Leach-Baily Act (GLB)) – 15 U.S.C. 6801 through 6827

Covered Personal Information

"Nonpublic personal information" defined as personally identifiable financial information:

- provided by a consumer to a financial institution;
- resulting from any transaction with the consumer or any service performed for the consumer; or
- otherwise obtained by the financial institution.[22]

Covered Entities

"Financial institutions" is defined as any institution the business of which is engaging in financial activities as described in a referenced federal code.[23]

The GLB specifically does not cover:

- businesses subject to the jurisdiction of the Commodity Futures Trading Commission under the Commodity Exchange Act (e.g., securities and investment companies);

[22] 15 U.S.C. 6809(4).

[23] 15 U.S.C 6809.

- farm credit institutions covered under the Federal Agricultural Mortgage Corporation or any entity chartered and operating under the Farm Credit Act of 1971; and

- companies that do not sell or transfer nonpublic personal information to nonaffiliated third party businesses.[24]

Individual Rights

Customers must be given:

- adequate notice about how the company uses personal information;

- the opportunity to direct that personal information not be disclosed to unaffiliated third parties; and

- an explanation of how to exercise that nondisclosure option.[25]

Exception:

- A financial institution need not provide a customer with the option for nondisclosure to an unaffiliated third party if the personal information is being given for:
    - marketing the financial institution's own products or services; or
    - marketing financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with certain requirements, if:
        - the financial institution fully discloses to the customer that it is providing the information; and
        - the financial institution enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of the information.[26]

Oversight and Enforcement

Regulation and enforcement authority is given to the following agencies within their respective areas of jurisdiction over the various types of financial institutions (e.g., banks, insurance providers, securities companies, etc.):

- Bureau of Consumer Financial Protection (created by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010);
- Federal Trade Commission;
- federal functional regulators; and
- state insurance authorities.[27]

[24] Ibid.
[25] 15 U.S.C. 6802.
[26] 15 U.S.C 6802(b).
[27] 15 U.S.C. 6805.

Fair Credit Reporting Act (15 U.S.C. 1681, et. seq.)

Covered Personal Information

Any information collected by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for services, products, or employment.[28] This information includes:

- basic identifying information, such as name, address, previous address, Social Security Number, marital status, employment information, and number of children;
- financial information, such as estimated income, employment, bank accounts, value of car and home;
- public records information, such as arrests, bankruptcies, and tax liens;
- lines of credit information, such as credit accounts and their status, such as payment habits on credit accounts;
- collection information, such as whether the person has unpaid or disputed bills;
- current employment and employment history;
- requests for a credit report, including the number of requests for the data and who requested the report;
- narrative information, such as a statement regarding disputed items on the credit report; and
- health information.[29]

Covered Entities

- Consumer reporting agencies, defined as:
  - an entity that assembles and sells credit information and financial information about individuals, such as Experian, Trans Union, and Equifax;

[28] 15 U.S.C. 1681a(d).

[29] Electronic Privacy Information Center, "The Fair Credit Reporting Act (FCRA) and the Privacy of Your Credit Report," web article at https://epic.org/privacy/fcra/, accessed on Nov. 13, 2015.

- smaller credit reporting agencies that usually concentrate on reporting on individuals living in certain regions of the country;
- inspection bureaus that sell information to insurance companies and assist in performing background checks;
- tenant screening and check approval companies; or
- depending on the nature of the operation, other companies or individuals that collect covered personal information, such as private investigators, detective agencies, collection agencies, and college placement offices.[30]

Individual Rights

- Consumers are granted the right to:
  - know what it is their credit reports;
  - be notified if information in their credit reports has been used to deny an application;
  - dispute incomplete, inaccurate, outdated information;
  - require information that a credit reporting agency cannot verify be removed or corrected;
  - consent before the credit report is given to an employer;
  - opt out when sent unsolicited "prescreening/prequalification" offers;
  - in some cases, sue in federal or state court if there has been a violation of rights;
  - additional rights are available to identity theft victims and military personnel.[31]

Oversight and Enforcement

- Individuals have a private right of action and may file civil lawsuits in federal or state courts.
- Fraud and other knowing and willful violations may result in criminal prosecution.
- Federal enforcement agencies that may regulate and handle complaints include:
  - FTC;
  - Department of the Treasury;
  - Federal Reserve;
  - National Credit Union Administration;

---

[30] Ibid.

[31] FTC, "A Summary of Your Rights Under the FCRA," document posted on the FTC web page at https://www.ftc.gov/news-events/media-resources/consumer-finance/credit-reporting, accessed on Nov. 13, 2015.

- Federal Deposit Insurance Corporation;
- Department of Transportation; and
- Department of Agriculture.

- Montana state enforcement agencies include:
  - Office of Consumer Protection, Department of Justice;
  - State Auditor's Office; and
  - Banking and Financial Institutions Division, Department of Administration.[32]

Health Insurance Portability and Accountability Act (HIPAA) – Pub. L. 104-191

Covered Personal Information

HIPAA contains definitions of the following types of information:

- Health information – broadest category of information - any information, whether oral or recorded in any form or medium, that is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual. [33]
  - Individually identifiable health information – a subset of "health information" - is health information that identifies the individual; or with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.[34]
    - Protected health information (PHI) – a subset of "individually identifiable health information" – it is individually identifiable health information that is held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral.[35]

[32] Ibid.

[33] HIPAA, Section 1171, subsection (4).

[34] HIPPA, Section 1171, subsection (6).

[35] HHS web page summary of HHS Privacy Rule under HIPPA, at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html.

Covered Entities

HIPAA covers the following entities:

- Health plans, including health insurance companies, HMOs, company health plans, and certain government programs that pay for health care, such as Medicare and Medicaid.

- Most health care providers—those that conduct certain business electronically, such as electronically billing your health insurance—including most doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacies, and dentists.

- Health care clearinghouses—entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

- Business associates of covered entities:
    - contractors, subcontractors, and other outside persons and companies that are not employees of a covered entity, such as:
        - billing companies;
        - companies that help administer health plans;
        - consultants or contracted lawyers, accountants, and IT specialists; and
        - companies that store or destroy medical records.[36]

Individual Rights

HIPAA allows patients to:

- ask to see and get a copy of their health records;
- correct their health information;
- receive a notice about how their health information may be used and shared;
- consent or not to the use or sharing of their health information for certain purposes, such as for marketing;
- obtain a report on when and why their health information was shared for certain purposes;
- file a complaint with a provider or health insurer if they believe their health information was not kept confidential; and
- file a complaint with HHS.[37]

In general, under the Privacy Rule, health information cannot be used or shared without written permission unless specifically allowed by law. For example, without a patient's authorization, a provider generally cannot give health information to person's employer, share the information for marketing or advertising purposes, or sell the information.

[36] Ibid.

[37] HHS web page summary of HHS Privacy Rule under HIPPA, http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/index.html.

The law allows health information to used and shared for the following reasons:

- treatment and care coordination;
- payment for services;
- with family, relatives, friends, or others identified by patients as involved with their health care or responsible for payment;
- for quality control;
- to protect the public's health; and
- to make required reports to law enforcement or as ordered by a court.[38]

Oversight and Enforcement

- Individuals do not have a private right of action to file a lawsuit.
- There are federal civil and criminal penalties for failure to comply with HIPAA.
- The Office of Civil Rights within HHS may:
    - investigate complaints;
    - impose certain civil penalties (fines);
    - conduct compliance reviews; and
    - conduct education and outreach.
- The U.S. Department of Justice is responsible for investigating and prosecuting possible criminal violations of HIPAA.
- The Centers for Medicare and Medicaid Services under HHS also has an oversight and enforcement role.[39]

Montana State Agencies

State agencies in Montana that have a key role with respect to personal information include:

- Office of Consumer Protection, Department of Justice;
- State Auditor's Office;
- Banking and Financial Institutions Division, Department of Administration;
- State Information Technology Services Division, Department of Administration; and
- Department of Public Health and Human Services.

[38] Ibid.

[39] HHS web page summary of enforcement and compliance under HIPAA, http://www.hhs.gov/ocr/privacy/hipaa/enforcement/process/index.html.

Montana Laws

Montana Unfair Trade Practices and Consumer Protection Act of 1973 - Title 30, ch. 14, part 1, MCA

Covered Information

- Similar to the Federal Trade Commission Act, the Montana Unfair Trade Practices and Consumer Protection Act of 1973 general protects consumers by prohibiting unfair or deceptive business practices. In fact, a specific statute states that it is the intent of the legislature that "that in construing 30-14-103 [Montana's prohibition] due consideration and weight shall be given to the interpretations of the federal trade commission and the federal courts relating to section 5(a)(1) of the Federal Trade Commission Act (15 U.S.C., 45(a)(1)), as amended. The statute also grants the Department of Justice authority to adopt rules interpreting what constitutes unfair or deceptive practices as long as the rules are not inconsistent with the FTC Act.[40]

- The Montana Act does not define "personal information". It defines "documentary material" as follows: "the original or a copy of any book, record, report, memorandum, paper, communication, tabulation, map, chart, photograph, mechanical transcription, or other tangible document or recording."[41]

Covered Entities

- Any person who conducts unfair or deceptive trade practices. "Person" is defined as "natural persons, corporations, trusts, partnerships, incorporated or unincorporated associations, and any other legal entity".[42]

Individual Rights

- A consumer has the right to bring a lawsuit for "any ascertainable loss of money or property, real or personal, as a result of the use or employment by another person" of an unfair or deceptive trade practice.[43]

Oversight and Enforcement

- As mentioned above, a consumer may bring a lawsuit in a district court.

- The Department of Justice may "bring an action in the name of the state against the person [it believes has perpetrated an unfair or deceptive trade practice] to restrain by

[40] Section 30-13-104, MCA.
[41] Section 30-13-102(3), MCA.
[42] Section 30-14-102(6), MCA.
[43] Section 30-14-133, MCA.

temporary or permanent injunction or temporary restraining order the use of the unlawful method, act, or practice upon giving appropriate notice to that person."[44]

- The Department of Justice may investigate complaints and compel the furnishing of information.

- County attorneys must "lend to the department the assistance that the department may request in the commencement and prosecution of actions pursuant to this part. The county attorney, on request of the department or another county attorney may initiate all procedures and prosecute actions in the same manner as provided for the department."[45]

Prohibition Against Unfair or Deceptive Trade Practices by Insurers - Section 33-18-102, MCA

This provision is similar to the Montana Unfair Trade Practices and Consumer Protection Act of 1973, as summarized above, except that it applies only to insurers and is related to a federal act specific to the insurance business.

Insurance Information and Privacy Protection Act - Title 33, ch. 19, MCA

Covered Information

- Personal information – any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocations, finances, occupation, general reputation, credit, health, or any other personal characteristics. Personal information includes an individual's name and address and medical record information but does not include privileged information.[46]

- Several subcategories of information are covered by special provisions, such as: medical information, consumer report information, privileged information, and recorded personal information.

Covered Entities

[44] Section 30-14-111, MCA.
[45] Section 30-14-121, MCA.
[46] 33-19-104(21), MCA.

- Certain insurance institutions, insurance producers, or insurance-support organizations that are not "covered entities" under HIPAA.

Individual Rights

- Must receive "clear and conspicuous" notice of information practices.
- Questions designed to gather personal information solely for marketing or research must be clearly specified.
- May request a copy of investigative consumer reports.
- May request access to recorded personal information.
- May request corrections, amendments, or deletions of recorded personal information.
- May request information specifying the reasons for an adverse underwriting decision.
- Consent is required before personal or privileged information may be disclosed.
- In certain circumstances, consent is required before personal information may be disclosed for marketing or research purposed.
- Notice of any security breach that has resulted in the disclosure of unencrypted personal information. For the purposes of the security breach notification provision, "personal information" is defined as a person's name and one or more of the following:
    - social security number;
    - driver's license, state, or tribal id number;
    - an account number;
    - medical record information;
    - taxpayer id number; or
    - an identity protection personal id number issued by the IRS.

Oversight and Enforcement

- Montana's Commission of Insurance (i.e., the State Auditor's Office) is empowered to
    - examine and investigate covered entities; and
    - impose fines.
- Harmed individuals have a private right of action (i.e., may file a civil lawsuit).
- The Attorney General or a county attorney may prosecute for criminal violations.

Impediment to identify theft provisions - Title 30, ch. 14, part 1, MCA

Covered Information

- "Personal information" is defined as "an individual's name, signature, address, or telephone number, in combination with one or more additional pieces of information about the individual, consisting of the individual's passport number, driver's license or state identification number, insurance policy number, bank account number, credit card number, debit card number, passwords or personal identification numbers required to

obtain access to the individual's finances, or any other financial information as provided by rule. A social security number, in and of itself, constitutes personal information."[47]

- For the purposes of the security breach notification section, "personal information" is defined as an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:
    - social security number;
    - driver's license number, state identification card number, or tribal identification card number;
    - account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account;
    - medical record information as defined in 33-19-104;
    - a taxpayer identification number; or an identity protection personal identification number issued by the United States internal revenue service.
    - Personal information does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.[48]

Covered Entities

- Businesses – a "business" is defined as "a sole proprietorship, partnership, corporation, association, or other group, however organized and whether or not organized to operate at a profit, including a financial institution organized, chartered, or holding a license or authorization certificate under the law of this state, any other state, the United States, or any other country or the parent or the subsidiary of a financial institution. The term includes an entity that destroys records. The term also includes industries regulated by the public service commission or under Title 30, chapter 10." [49]

- Businesses regulated under Title 33 (insurance companies) are not covered.

- Internet services providers – defined as "a person or an entity that provides a service, available to the public, that enables the person's or entity's customers to access the internet, purchase internet server or file-hosting services, colocate internet equipment, or use data transmission over the internet for a fee."[50]

---

[47] Section 30-14-1702(7), MCA.
[48] Section 30-14-1704(4)(b),MCA.

[49] Section 30-14-1702(1), MCA.
[50] Section 2-17-602, MCA.

Individual Rights

There is a private right of action allowing a harmed individual to file a civil lawsuit.[51]

Oversight and Enforcement

- Montana Department of Justice may issue subpoenas, administer oaths, conduct hearings, prescribe forms, and adopt rules[52] and may also bring an action in the name of the state against a person violating the statutes to stop the practices violating the statutes.[53]
- County attorneys must assist the department and may prosecute violations.[54]
- Civil fine. [55]
- Criminal penalty for fraud. [56]

State Agency Protection of Personal Information - Title 2, ch. 6, part 15, MCA

Covered Information

- "Personal information", which is defined as "a first name or first initial and last name in combination with any one or more of the following data elements when the name and data elements are not encrypted:
  - a social security number;
  - a driver's license number, an identification card number issued pursuant to 61-12-501, a tribal identification number or enrollment number, or a similar identification number issued by any state, the District of Columbia, the Commonwealth of Puerto Rico, Guam, the Virgin Islands, or American Samoa;
  - an account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to a person's financial account;
  - medical record information as defined in 33-19-104;
  - a taxpayer identification number; or
  - an identity protection personal identification number issued by the United States internal revenue service.[57]

[51] Section 30-14-133, MCA.
[52] Section 30-14-114, MCA.
[53] Section 30-14-1705, MCA.
[54] Section 30-14-121, MCA.
[55] Section 30-14-1705, MCA.
[56] Ibid.
[57] Section 2-16-1501(4), MCA.

Governmental Internet Information Privacy Act – Title 2, ch. 17, part 5 (sections 2-17-550 through 553), MCA

Covered Information

- Personally identifiable information collected online - individually identifiable information is defined as:
  - a first and last name;
  - a residence or other physical address, including a street name and name of a city or town;
  - an e-mail address;
  - a telephone number;
  - a social security number; or
  - unique identifying information that an internet service provider or a government website operator collects and combines with any information described above.[58]

Covered Entities

- Governmental entities – defined as state and political subdivisions of the state (county, city, municipal corporation, school district, or other political subdivision or public corporation) – that have websites.[59]

Individual Rights

- Users of governmental entity websites are entitled to:
  - know who operates the website;
  - the address and telephone number at which the website operator may be contacted as well as an electronic means for contacting the operator; and
  - be given a general description of the operator's information practices, including policies to protect the privacy of the user and the steps taken to protect the security of the collected information.[60]

- If personally identifiable information may be used for a purpose other than the express purpose of the website or may be given or sold to a third party, except as required by law, then the website operator shall ensure that the website includes:
  - a clear and conspicuous notice to the user that the information collected could be used for other than the purposes of the website;
  - a general description of the types of third parties that may obtain the information; and

[58] Section 2-17-551(6), MCA.

[59] Section 2-17-551, MCA.

[60] Section 2-17-552, MCA.

- a clear, conspicuous, and easily understood online procedure requiring an affirmative expression of the user's permission before the information is collected.[61]

Oversight and Enforcement

There is no provision within these three sections of statutes that specify oversight duties or reference penalty provisions for a violation of provisions contained in the three sections. However, the Chief Information Office and the State Information Technology Services Division have broad duties and certain enforcement authority regarding ***state agency*** information technology policies and standards.

Uniform Health Care Information Act – Title 50, Ch. 16, Part 5.

Covered Information

- "Health information" means any information, whether oral or recorded in any form or medium, that identifies or can readily be associated with the identity of a patient and relates to the patient's health care. The term includes any record of disclosures of health care information.[62]

Covered Entities

- "Health care provider" means a person who is licensed, certified, or otherwise authorized by the laws of this state to provide health care in the ordinary course of business or practice of a profession.[63]

- Applies only to a health care provider that is not subject to the privacy provisions of HIPAA and administrative rules adopted in connection with HIPAA.[64]

Individual Rights

- Patient must receive notice of provider's health information practices.[65]
  - disclosure to a person who has a "need to know" as prescribed by state law (see section 50-16-529, MCA);
  - disclosure under section 50-16-530, MCA, for:
    - directory information, unless a patient specifically requests the provider to not make the disclosure;
    - for public health and safety if the provider is required by law to disclose the information;

[61] Ibid.

[62] Section 50-16-504(6), MCA.

[63] Section 50-16-504(7), MCA.

[64] Section 50-16-505, MCA.

[65] Section 5-16-512, MCA.

- law enforcement purposes, but only certain information and only under specified circumstances;
- response to a certain type of request from the office of victims services;
- when compelled by a court or any judicial, legislative, or administrative proceeding, except as listed in section 50-16-535, MCA, and in compliance with section 50-16-536, MCA.

- Patients may revoke authorization to disclose their health information.[66]
- Patients may examine, copy, and submit corrections to their health information.[67]

Oversight and Enforcement

Criminal and civil penalties are provided for in statute and the state attorney general or a county attorney is authorized to prosecute violations.[68]

Government Health Care Information Act – Title 50, Chapter 16, Part 6.

Covered Information

- "Health care information" means information, whether oral or recorded in any form or medium that identifies or can readily be associated with the identity of an individual, including one who is deceased, and that relates to that individual's health care or status. The term includes any record of disclosures of health care information and any information about an individual received pursuant to state law or rules relating to communicable disease. The term does not include vital statistics information gathered under Title 50, chapter 15.[69]

Covered Entities

- Department of Public Health and Human Services.
- Local health board of a city, county, city-county, or district.
- Local health officer appointed by a local health board.
- However, if the entity is covered by the Uniform Health Care Information Act under Part 5, the entity is subject to that Act and not the Government Health Care Information Act under Part 6.[70]

Individual Rights

[66] Section 50-16-528, MCA.
[67] Sections 50-16-512, 50-16-541 through 50-16-545, MCA.
[68] Sections 50-16-551 through 50-16-553, MCA.
[69] Section 50-16-602(2), MCA.
[70] Section 50-16-602(1), (3), and (4), MCA, and section 50-16-606, MCA.

- Individual must specifically and in writing authorize disclosure, except the information may disclosed for:
    - statistical purposes when not identification of individuals can be made from the disclosure;
    - medical emergencies;
    - as evidence in a child protective services or child abuse and neglect court proceeding, but the court must seal the records at the conclusion of the proceeding; or
    - if necessary to implement or enforce laws or rules concerning the prevention and control of certain diseases.[71]

Oversight and Enforcement

- A criminal penalty (a misdemeanor, which is enforced by a county attorney) is provided for that requires a fine and jail time for a person convicted of knowingly violating a provision of the Act.[72]

Health Care Information Privacy Requirement for Providers Subject to HIPAA – Title 50, Chapter 16, Part 8

Covered Information

- "Health care information" means any information, whether oral or recorded in any form or medium, that is:
    - created or received by a health care provider;
    - relates to the past, present, or future physical or mental health or condition of an individual or to the past, present, or future payment for the provision of health care to the individual; **and**
    - identifies or with respect to which there is a reasonable basis to believe the information can be used to identify the individual.[73]

Covered Entities

- "Health care provider" means a person who is licensed, certified, or otherwise authorized by the laws of this state to provide health care in the ordinary course of business or practice of a profession.[74]
- Applies only to “health care providers” covered by HIPAA.[75]

Individual Rights

[71] Section 50-16-603, MCA.
[72] Section 50-16-611, MCA.
[73] Section 50-16-803(3), MCA.
[74] Section 50-16-803(4), MCA.
[75] Section 50-16-802, MCA.

- The statutes are written in such a way that the information may not be disclosed except as specifically described in the statutes.
  - Most of the conditions under which the information may be released do not involve the patient's authorization or exercise of a right to control the information.
  - However, the patient may:
    - authorize in writing the release of the information in response to a compulsory process or a discovery request; or
    - waive the right to claim confidentiality.[76]

Oversight and Enforcement

- A person aggrieved by a violation of these statutes may file a civil lawsuit.
- A court may order compliance and appropriate relief (but the statute defines the maximum fine provides a statute of limitations).
- There are protections for whistle blowers.[77]

Other States

Many states are taking on the issue of personal data protection, ownership, and digital privacy.[78] According to the National Conference for State Legislatures (NCSL):

- In October 2015, California, which is considered a bellwether state regarding privacy and personal information laws, enacted the Electronic Communications Privacy Act (the California ECPA). Providing stricter protections that the federal ECPA, the California ECPA requires, with some exceptions, that state governmental entities get a search warrant before obtaining or accessing electronic information stored on smartphones, tablets, laptops and other electronic devices. The electronic information includes e-mail, digital documents, photographs, passwords, geolocation data, and internet protocol (IP) addresses, which identify individual computers.[79]

[76] Sections 50-16-805 and 50-16-811, MCA.

[77] Section 50-16-817, MCA.

[78] The National Conference of State Legislatures (NCSL) maintains a web page with information about information privacy and security laws in other states: http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-and-security.aspx.

[79] Goodwin Procter LLP, "California Enacts CalECPA," Client Alert, Oct. 14, 2015, available at http://www.goodwinprocter.com/Publications/Newsletters/Client-Alert/2015/10_14-California-Enacts-CalECPA-Requiring-a-Search-Warrant-to-Obtain-or-Access-Users-Electronic.aspx.

- In 2013, legislatures in 36 states considered legislation prohibiting employers or educational institutions from requiring employees, applicants, or students to provide passwords to their social media accounts. By April 2014, 28 states had passed legislation in this area.[80]

- At least 19 states have laws restricting the collection, use, disclosure, or sharing of biometric data (e.g., finger prints, retinal scans, facial scans, vocal scans, DNA, etc.) by public or private entities; and at least 20 states have laws protecting personal biometric information of students or minors.[81]

- So far in 2015, at least 32 state legislatures have considered or enacted legislation concerning notification about security breaches.[82]

- Several states have prohibited web sites from "charging fees for the removal of mug shots from a web site or otherwise regulating these sites' practices. Georgia, Illinois, Oregon, Texas and Utah in 2013 enacted legislation to address these concerns by prohibiting commercial sites from charging fees for removing inaccurate mug shots upon request or by prohibiting sheriffs from releasing mug shots to sites that charge a fee, among other provisions. Legislation was enacted in California, Colorado, Georgia, Missouri and Wyoming in 2014, and in Maryland and Virginia in 2015."[83]

- The state of Delaware recently enacted four bills protecting the privacy of website and mobile application users, minors, students and crime victims.

---

[80] Pam Greenberg, "Social Media Privacy Laws," *LegisBrief*, National Conference for State Legislatures, Vol. 22, No. 16, April 2014.

[81] Pam Greenberg, "Facial Recognition and Biometrics," *LegisBrief*, National Conference for State Legislatures, Vol. 23, No. 41, Nov. 2015.

[82] National Conference for State Legislatures, Telecommunications and Information, Privacy and Security Web Pages, posted Oct. 22, 2015, at http://www.ncsl.org/research/telecommunications-and-information-technology/2015-security-breach-legislation.aspx.

[83] National Conference for State Legislatures, Telecommunications and Information, Privacy and Security Web Pages, posted Oct. 9, 2015, at http://www.ncsl.org/research/telecommunications-and-information-technology/mug-shots-and-booking-photo-websites.aspx.

Conclusion

This report has highlighted that with respect to personal information:

- There are a variety of federal and state laws and agencies involved in governing the control of personal information.

- Most federal laws and Montana's laws seem to approach personal information in the context of privacy and security.

- Definitions of personal information vary depending on the industry or activity covered by the law.

- Individual rights with respect to the laws summarized above generally involve the right to know a business's information policies, know what information a business has about the individual, correct errors, and consent to certain disclosures.

- States vary in how they approach governance of personal information. Approaches encompass a wide range of policy topics. California is a bellwether state for more restrictive laws that provided federally.