

# **HJR 21 Study Of Personal Information Ownership**

## **PROPERTY RIGHTS THEORY, POLICY PRINCIPLES, AND OPTIONS FOR FURTHER RESEARCH**

Prepared by Sheri Scurr, Research Analyst  
Montana Legislative Services Division

For the  
*State Administration and Veterans' Affairs Interim Committee*

February 10, 2016

---

**HJR 21 Study**  
**Personal Information Ownership:**  
**Property Rights Theory, Policy Principles, and**  
**Options for Further Research**

Prepared by Sheri Scurr, Research Analyst  
Montana Legislative Services Division

For the  
*State Administration and Veterans' Affairs Interim Committee*  
February 2016

---

## **Study Task**

The first study task for the State Administration and Veterans' Affairs Interim Committee under its adopted study plan for House Joint Resolution 21 (2015) is to "clarify the level of ownership that individuals have concerning the collection, dissemination, and use of personal data and the methods by which individuals may exercise and enforce their rights regarding use of that information."<sup>1</sup>

Two statements in the preamble for HJR 21 suggest that the committee should conceptualize this task as an examination of a bundle of property rights. These statements are:

WHEREAS, finding measures to conceptualize and legislate property rights regarding personal information will allow individuals to better control the collection, dissemination, and use of that information; and

WHEREAS, property rights are commonly conceptualized as a bundle of rights including the right to use a good, the right to earn income from a good, the right to transfer a good to others, and the right to enforcement of property rights.

## **Study Objective**

The objective outlined in HJR 21 is for the committee to develop recommendations regarding the collection, dissemination, and use of personal information that "will allow individuals to exercise and enforce their rights". This objective is premised on the notion that the individual is the center of the personal information ecosystem.

---

<sup>1</sup> 64th Montana Legislature, House Joint Resolution 21, subsection (2), 2015.

However, a review of literature and legal analysis in this area reveals that this premise is not agreed on by all stakeholders within this ecosystem.

## **Report Overview**

This report is divided into three parts and seeks to help the committee fulfill its study task and objective by:

- first, summarizing the legal theories and models that support conceptualizing personal information as property and defining levels of ownership based on a bundle of delegated rights;
- second, outlining the policy principles arising from these theories and models; and
- third, offering general options for how the committee may approach further study aimed at translating these principles into Montana law.

## **Word of Caution**

The property rights legal theory as a model for defining ownership and control of personal information does not seem to be widely accepted as a workable framework for developing laws. Nevertheless, even though legal scholars may disagree with various aspects of the property rights theory, most seem to agree that the current framework, which consists of a patchwork sector-specific privacy and security laws, offers insufficient protections for individual rights. Thus, there is general agreement that more should be done to allow individuals greater control over the collection, use, and dissemination of their personal information.<sup>2</sup>

---

<sup>2</sup> Jane B. Baron, "Property as Control: The Case for Information", 18 *Michigan Telecommunications and Technology Law Review*, 367 (2012). See also, Barbara J. Evans, "Much Ado About Data Ownership", *Harvard Journal of Law & Technology*, Vol. 25, No. 1, Fall 2011. See also, Jessica Litman, "Information Privacy/Information Property", 52 *Stanford Law Review* 1283, 1999-2000.

---

## **PART 1 -**

# **THE PROPERTY RIGHTS LEGAL THEORY**

---

### **Defining Ownership**

#### **Individuals own their personal data**

The property rights ownership model for regulating the use and distribution of personal information is built on the following premise: "People should own information about themselves, and, as owners of property, should be entitled to control what is done with it."<sup>3</sup>

#### **Ownership is delegated when data is shared**

One advocate for this theory, Ali M. Al-Khouri, an internationally recognized scholar, defines "personal data" as information a person uses to identify themselves for personal gain, whether that gain is physical (e.g., financial, material, or medical), intellectual (e.g., for writing and research), or emotional (e.g., communicating and social networking). His argument is that when an individual shares his or her personal data, the person is delegating ownership. Thus, after the data is shared, there is another owner. Furthermore, Al-Khouri argues, each time the data is analyzed and shared again, the data is converted to new information and new levels of ownership are created.<sup>4</sup>

#### **Ownership is delegated in different ways**

Al-Khouri outlines three ways in which personal data is shared and ownership is delegated:

- When it is volunteered by the individual.
- When it is captured by an entity recording an individual's activities.
- When it is discerned through analysis.<sup>5</sup>

---

<sup>3</sup> Jessica Litman, "Information Privacy/Information Property", 52 *Stanford Law Review* 1283, 1999-2000, p. 2056.

<sup>4</sup> Ali M. Al-Khouri, "Data Ownership: Who Owns 'My Data'?", *International Journal of Management & Information Technology*, Vol. 2, No. 1, November 2012. Available at [www.ijmit.com/](http://www.ijmit.com/) ISSN: 2278-5612.

<sup>5</sup> Ibid.

Paul M. Schwartz, another legal scholar and one of the first prominent advocates for approaching personal information as property, characterizes this sharing of personal information as a "market transaction" and likens personal information as a currency in this era of big data.<sup>6</sup>

## **Different ways to define ownership**

### **Verifier of accuracy is owner**

Under Al-Khouri's theory, the owner of the personal information is determined by identifying who can verify the accuracy of the information. In other words, whomever can verify the accuracy of the information, owns the information. For example, Al-Khouri argues, Google doesn't own an individual's Internet search, but does own the results of the company's analysis of the individual's Internet search patterns.<sup>7</sup>

### **Analyzed information is no longer owned by individual**

Other legal scholars have discussed this property rights theory in the context of individual health records and argue that information ownership as similar to the commonly accepted view of property ownership as a "bundle of rights". They argue that each right may be separated from the bundle and treated individually. These scholars note that there are laws already in place stating that an individual's health information is owned by that individual, but that the medical analysis, conclusions, and recommendations along with the physical method of recording and storing the information is owned by the service provider.<sup>8</sup>

Portions of the information ownership theory also seem to be currently applied in the context of financial transactions. The individual is recognized as the owner of the personal information shared by the individual when conducting financial transactions, but the individual does not own his or her credit score.

---

<sup>6</sup> Paul M. Schwartz, "Property, Privacy, and Personal Data", 117 *Harvard Law Review* 2056, 2003-2004.

<sup>7</sup> Al-Khouri, p.4.

<sup>8</sup> Barbara J. Evans, "Much Ado About Data Ownership", *Harvard Journal of Law & Technology*, Vol. 25, No. 1, Fall 2011. See also Jane B. Baron, "Property As Control: The Case Of Information", 18 *Michigan Telecommunications and Technology Law Review* 367, 2012, pp. 384-385.

The credit score is generated by a credit agency as a result of the agency's proprietary analysis of that personal information. Therefore, the credit agency owns the credit score.<sup>9</sup>

### **Some ownership is inalienable**

Schwartz describes the levels of ownership a bit differently than Al-Khoury. He argues that there is a degree of inalienability in the sharing of personal information. In other words, an individual cannot consent to giving up all of his or her ownership interest in the information because individuals have an inalienable (i.e., natural) right to "selfhood". Under Schwartz's inalienability theory, even though some ownership may be delegated when the information is shared, there are limits to how much ownership can be delegated. Quoting other legal scholars, Schwartz argues that property is an interest that 'runs with the asset' and that this limits the ownership interests of third-parties downstream of the first transaction.<sup>10</sup>

## **Contrasting Privacy and Property Theory**

### **A balancing act**

Advocates of the property rights legal theory do not entirely abandon the privacy rights approach to regulation of how personal information is collected, used, and disseminated.

In presenting his model for "propertized personal information", Schwartz acknowledges the shortcomings of a pure property rights approach. He notes:

Legal scholars interested in protecting information privacy, however, have been suspicious of treating personal data as a form of property and have generally advocated imposing a ban on data trade, rather than restrictions on transferability. In contrast, other legal scholars have advocated propertization of personal information, albeit generally without sufficient sensitivity to privacy concerns.<sup>11</sup>

Schwartz attempts to balance these contrasting views by acknowledging that laws protecting information privacy have provided a framework for limiting the use, transfer, and processing of personal data, but he argues this framework does not recognize that personal information is a traded commodity in the "big

---

<sup>9</sup> Al-Khoury, p. 3.

<sup>10</sup> Schwartz, p. 2097.

<sup>11</sup> Ibid., p. 2057

data" economy and that this commodity would not have any value without the choices of the first owner of the property, the individual. He urges privacy rights scholars to acknowledge and protect individual ownership rights. In return, he assures that his propertization model will "fully safeguard information privacy".<sup>12</sup>

### **European view is different than America's view**

Some analysts say that European countries have been able to successfully regulate corporate behavior under the privacy rights model because privacy is viewed differently under European law than it is in the United States.

Bob Sullivan, an MSNBC.com technology consultant, sums up this difference between the United States and Europe as follows:

The reason that privacy laws in Europe and the U.S. are so different springs from a basic divergence in attitude: Europeans reserve their deepest distrust for corporations, while Americans are far more concerned about their government invading their privacy.

As a result, U.S. federal agencies have been given little power to limit the potentially privacy-invading behaviors of private companies. The Federal Trade Commission, the agency charged with protecting U.S. citizens from such intrusions, rarely acts against U.S. firms. When it does, its remedies are generally limited to small fines and out-of-court settlements.

Each European nation, on the other hand, has its Data Protection Authority to monitor corporate behavior. Consumers can appeal to the authority, which in some countries boasts far-ranging subpoena power. Fines for misbehavior are common.<sup>13</sup>

Sullivan acknowledges that the European approach is not without its critics. He quotes a privacy lawyer who says that the regulations in Europe constitute "unmanageable red tape" and have become so cumbersome that many companies risk noncompliance in order to stay competitive.<sup>14</sup>

---

<sup>12</sup> Schwartz, p. 2058.

<sup>13</sup> Bob Sullivan, "La difference is stark in EU, U.S. privacy laws", Privacy Lost series on NBC News.com at [www.nbcnews.com/id/15221111/ns/technology\\_and\\_science-privacy\\_lost/t/la-difference-stark-eu-us-privacy-laws/#.VpV0602FPD](http://www.nbcnews.com/id/15221111/ns/technology_and_science-privacy_lost/t/la-difference-stark-eu-us-privacy-laws/#.VpV0602FPD).

<sup>14</sup> Ibid.

## **What matters is the result**

Legal scholar Jane B. Baron is critical of the property ownership model and "bundle of rights" approach to defining ownership and control. However, she does concede it could be an appropriate approach to the sharing of individual health information. Thus, Baron concludes that in the final analysis it is immaterial whether one invokes privacy rights or property rights. "What matters," she says, "is the values ultimately served by whatever package of rights is put together."<sup>15</sup>

[go to next page]

---

<sup>15</sup> Baron, p. 389.



---

## **PART 2 -**

# **POLICY PRINCIPLES**

---

### **Overview**

Various sets of principles have been developed internationally and nationally and offered as a framework to guide policymaking. Some of these sets of principles are outlined below.<sup>16</sup>

These principles may help lay a foundation for the committee to fulfill its study objective and develop recommendations regarding the collection, dissemination, and use of personal information.<sup>17</sup>

### **Safe Harbor Model - An International Agreement**

#### **Background**

In 1995, the European Union adopted a directive (updated by a European Commission decision in 2001)<sup>18</sup> concerning the transfer of personal data about EU citizens to entities in other countries. The directive articulated a set of seven non-binding principles first recommended by the international Organization for Economic Cooperation and Development in 1980.<sup>19</sup>

Between 1998 and 2000, the United States and the European Union developed what was termed the "Safe Harbor Privacy Principles" as a set of voluntary standards designed to protect personal information from being inappropriately disclosed. In a decision called the "Safe Harbor Decision", the European Commission decided that U.S. companies could transfer personal data from the

---

<sup>16</sup> The summaries presented in this part are based on review of the various materials researched for this report. The labels for the models are creations of the author of this report.

<sup>17</sup> 64th Montana Legislature, HJR 21 (2015).

<sup>18</sup> 2001/497/EC: Commission Decision of 15 June 2001, accessed in January 2016 at <http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001D0497>.

<sup>19</sup> Wikipedia, "International Safe Harbor Privacy Principles", accessed in January 2016 at [https://en.wikipedia.org/wiki/International\\_Safe\\_Harbor\\_Privacy\\_Principles](https://en.wikipedia.org/wiki/International_Safe_Harbor_Privacy_Principles).

European Union to the United States if the companies self-certified their compliance with the seven Safe Harbor Privacy Principles and registered themselves with the U.S. Federal Trade Commission.<sup>20</sup>

In 2012, the European Commission embarked on a comprehensive reform of its data privacy laws and is still working toward enacting a single comprehensive law "to give citizens back control over of their personal data, and to simplify the regulatory environment for business."<sup>21</sup>

## **Current status**

However, in October 2015, the European Court of Justice declared invalid the European Commission's decision in 2000 that the Safe Harbor framework negotiated with the United States government provided adequate privacy protections. On Nov. 6, 2015, the Federal Trade Commission posted the following notice on its Web site:

### **Update on the U.S.-EU Safe Harbor Framework**

On October 6, 2015, the European Court of Justice issued a judgment declaring as invalid the European Commission's Decision 2000/520/EC of 26 July 2000 on the adequacy of the U.S.-EU Safe Harbor Framework. U.S. and EU officials are currently discussing the development of an enhanced mechanism that protects privacy and provides an alternative method for transatlantic data transfers. In the meantime, we continue to expect companies to comply with their ongoing obligations with respect to data previously transferred under the Safe Harbor Framework. We also encourage companies to continue to follow robust privacy principles, such as those underlying the Safe Harbor Framework, and to review their privacy policies to ensure they describe their privacy practices accurately, including with regard to international data transfers. Updated: November 6, 2015.

---

<sup>20</sup> Jan Dhont, Maria Veronica Perez Asinari, and Yves Poullet, "Safe Harbour Decision Implementation Study," European Commission, Internal Market DG Contract PRS/2003/A0-7002/E/27, April 19, 2004.

<sup>21</sup> European Commission Web site under the data protection topic at [http://ec.europa.eu/justice/data-protection/index\\_en.htm](http://ec.europa.eu/justice/data-protection/index_en.htm).

## **Seven principles**

The seven Safe Harbor principles are as follows:

1. **Notice** - Individuals must be informed that their data is being collected and about how it will be used.
2. **Choice** - Individuals must have the option to opt out of the collection and the forward transfer of the data to third parties.
3. **Onward Transfer** - Transfers of data to third parties may only occur to other organizations that follow adequate data protection principles.
4. **Security** - Reasonable efforts must be made to prevent loss of collected information.
5. **Data Integrity** - Data collected and transferred must be relevant and reliable and used only for the purpose it was collected for.
6. **Access** - Individuals must be able to access information held about them, and correct or delete it if it is inaccurate.
7. **Enforcement** - There must be effective means of enforcing these rules.<sup>22</sup>

## **Schwartz Model - A Bundle of Interests**

Schwartz also presents a set of principles to guide policymaking concerning personal information use and dissemination. He sums up his principles as follows:

...I suggest that the understanding of property as a bundle of interests rather than despotic dominion over a thing helps frame a viable system of rights with respect to personal data. Moreover, these property interests are to be shaped through legal attention to five areas: inalienabilities, defaults, a right of exit, damages, and institutions.<sup>23</sup>

---

<sup>22</sup> 2000/520/EC: Commission Decision of 26 July 2000 available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML>

<sup>23</sup> Schwartz, p. 2094.

Schwartz's arguments concerning these five areas may be outlined as follows:

- 1. Opt-in requirement** - For companies to have the right to use and disseminate personal information, the individual should have to take an affirmative action (i.e., the policy should be to require an "opt-in" selection, not to allow a person to "opt-out").
- 2. Transparency** - Policies on the use and dissemination of personal information should be fully disclosed and practices should be transparent.
- 3. Verifiable compliance** - Individuals, data collectors, data users, and data brokers should be able to verify that those companies receiving the information have also complied with opt-in, disclosure, and use policies.
- 4. Right of exit** - Individuals should have a "right of exit". In other words, even after an initial opt-in, an individual should be able to revoke that consent and opt out at any time.
- 5. Penalties** - Violators of these policies or standards should be penalized.
- 6. Enforcement** - Institutions should have oversight responsibilities and enforcement powers. Individuals should have the right to sue.

## **Al-Khouri Model - An Ownership Delegation Ecosystem**

Al-Khouri also offers a set of principles on which he believes national and international laws concerning data ownership should be based. He states that his goal in advocating for these principles is to "raise awareness and trigger a debate for policy makers with regard to data ownership and the need to improve existing data protection, privacy laws, and legislation at both national and international levels."<sup>24</sup>

The table on the following page is taken directly from Al-Khouri's article.<sup>25</sup>

---

<sup>24</sup> Al-Khouri, p. 1.

<sup>25</sup> Ibid., p. 5.

<b>Guiding Principle</b>	<b>Description</b>
<b>Accountability</b>	Organizations need to be held accountable for appropriate security mechanisms designed to prevent theft and unauthorized access of personal data, as well as for using data in a way that is consistent with agreed upon rules and permissions. They need to have the benefit of “safe harbor” treatment and insulation from open-ended liability, when they can demonstrate compliance with objectively testable rules that hold them to account.
<b>Enforcement:</b>	Mechanisms need to be established to ensure organizations are held accountable for these obligations through a combination of incentives, and where appropriate, financial and other penalties, in addition to legislative, regulatory, judicial, or other enforcement mechanisms.
<b>Data permissions:</b>	Permissions for usage need to be flexible and dynamic to reflect the necessary context and to enable value-creating uses, while weeding out harmful uses. Permissions also need to reflect that many stakeholders— including but not limited to individuals—have certain rights to use data.
<b>Balanced stakeholder roles:</b>	Principles need to reflect the importance of rights and responsibilities for the usage of personal data and strike a balance between the different stakeholders—the individual, the organization, and society. They also need to reflect the changing role of the individual from a passive data subject to an active stakeholder and creator of data. One perspective that is gathering momentum, though it is far from being universally accepted, is that a new balance needs to be struck that features the individual at the center of the flow of personal data, with other stakeholders adapting to positions of interacting with people in a much more consensual, fulfilling manner.
<b>Anonymity and identity:</b>	The principles need to reflect the importance of individuals being able to engage in activities online anonymously, while at the same time establishing mechanisms for individuals to effectively authenticate their identity in different contexts, so as to facilitate trust and commerce online.
<b>Shared data commons:</b>	The principles should reflect and preserve the value to society from the sharing and analysis of anonymised data sets as a collective resource.

## **Wang Model - A Compact With Consumers**

R. "Ray" Wang, a business analyst writing for the *Harvard Business Review* in 2013, argues that data-dependent businesses will not be able to build a sustainable relationship with consumers unless they follow basic rules of good behavior that allow customers to take back control of their data.<sup>26</sup>

Wang lists and explains in the follow way seven basic protections that consumers should demand and that businesses should voluntarily agree to do:

- 1. Make "opt-in" the default.** Basic profile information should require an affirmative permission to share information, use for offer creation, or even suggest next best action. Opt-ins should also apply to user-generated information such as messages, photos, audio, and video.
- 2. Be transparent in how personal information is used.** Organizations should detail what information will be shared. Users should know if their information will be sold and if so to whom.
- 3. Give advance notice of privacy changes.** Organizations should provide adequate warning when new features impact a user's privacy preferences.
- 4. Require "opt-in" for privacy changes.** The default option should be to keep privacy preferences the same. The recent Electronic Privacy Information Center FTC complaint and settlement with Facebook reinforces this principal.
- 5. Prevent access to user's data upon account deletion.** Information about a user should be locked down when an account is deleted. It should not be used in aggregate statistics or data.
- 6. Allow users to export their data.** Customers should own their data and be able to take it with them as needed. Doc Searls and the Project VRM community have been advocating Personal Data Stores for quite some time. This may be the necessary requirement for social business to make it to the next level.

---

<sup>26</sup> R. "Ray" Wang, "Beware Trading Privacy for Convenience," *Harvard Business Review*, June 10, 2013.

- 7. Give users a “hard delete” option.** Users should be able to request and receive a permanent deletion of their data, with all information removed from all files.<sup>27</sup>

## **Obama Administration Model - A Consumer Bill of Rights**

In February 2012, President Obama released a set of principles he called a consumer bill of rights and offered it as a blue print on which federal law could be based to protect consumers' control over their personal information but still allow for a dynamic global digital economy. In his introduction to the report, President Obama stated:

I am pleased to present this new Consumer Privacy Bill of Rights as a blueprint for privacy in the information age. These rights give consumers clear guidance on what they should expect from those who handle their personal information, and set expectations for companies that use personal data. I call on these companies to begin immediately working with privacy advocates, consumer protection enforcement agencies, and others to implement these principles in enforceable codes of conduct. My Administration will work to advance these principles and work with Congress to put them into law. With this Consumer Privacy Bill of Rights, we offer to the world a dynamic model of how to offer strong privacy protection and enable ongoing innovation in new information technologies.<sup>28</sup>

The bill of rights report presented the following principles as a basis for federal legislation to provide individuals with greater control over their personal information while still promoting a strong digital economy:

- 1. Individual Control** - Consumers have a right to exercise control over what personal data companies collect from them and how they use it. Companies should provide consumers appropriate control over the personal data that consumers share with others and over how companies collect, use, or disclose personal data. Companies should enable these choices by providing consumers with easily used and

---

<sup>27</sup> Ibid., pp. 3-4.

<sup>28</sup> "Consumer Data Privacy in the Internet World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy", The White House, February 2012, Barak Obama, introduction letter accessed in January 2016 online as a downloadable PDF from [www.whitehouse.gov](http://www.whitehouse.gov), under the issues search topic of "privacy".

accessible mechanisms that reflect the scale, scope, and sensitivity of the personal data that they collect, use, or disclose, as well as the sensitivity of the uses they make of personal data. Companies should offer consumers clear and simple choices, presented at times and in ways that enable consumers to make meaningful decisions about personal data collection, use, and disclosure. Companies should offer consumers means to withdraw or limit consent that are as accessible and easily used as the methods for granting consent in the first place.

- 2. Transparency** - Consumers have a right to easily understandable and accessible information about privacy and security practices. At times and in places that are most useful to enabling consumers to gain a meaningful understanding of privacy risks and the ability to exercise Individual Control, companies should provide clear descriptions of what personal data they collect, why they need the data, how they will use it, when they will delete the data or de-identify it from consumers, and whether and for what purposes they may share personal data with third parties.
- 3. 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. Companies should limit their use and disclosure of personal data to those purposes that are consistent with both the relationship that they have with consumers and the context in which consumers originally disclosed the data, unless required by law to do otherwise. If companies will use or disclose personal data for other purposes, they should provide heightened Transparency and Individual Control by disclosing these other purposes in a manner that is prominent and easily actionable by consumers at the time of data collection. If, subsequent to collection, companies decide to use or disclose personal data for purposes that are inconsistent with the context in which the data was disclosed, they must provide heightened measures of Transparency and Individual Choice. Finally, the age and familiarity with technology of consumers who engage with a company are important elements of context. Companies should fulfill the obligations under this principle in ways that are appropriate for the age and sophistication of consumers. In particular, the principles in the Consumer Privacy Bill of Rights may require greater protections for personal data obtained from children and teenagers than for adults.



- 4. Security** - Consumers have a right to secure and responsible handling of personal data. Companies should assess the privacy and security risks associated with their personal data practices and maintain reasonable safeguards to control risks such as loss; unauthorized access, use, destruction, or modification; and improper disclosure.
- 5. 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. Companies should use reasonable measures to ensure they maintain accurate personal data. Companies also should provide consumers with reasonable access to personal data that they collect or maintain about them, as well as the appropriate means and opportunity to correct inaccurate data or request its deletion or use limitation. Companies that handle personal data should construe this principle in a manner consistent with freedom of expression and freedom of the press. In determining what measures they may use to maintain accuracy and to provide access, correction, deletion, or suppression capabilities to consumers, companies may also consider the scale, scope, and sensitivity of the personal data that they collect or maintain and the likelihood that its use may expose consumers to financial, physical, or other material harm.
- 6. Focused Collection** - Consumers have a right to reasonable limits on the personal data that companies collect and retain. Companies should collect only as much personal data as they need to accomplish purposes specified under the Respect for Context principle. Companies should securely dispose of or de-identify personal data once they no longer need it, unless they are under a legal obligation to do otherwise.
- 7. 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. Companies should be accountable to enforcement authorities and consumers for adhering to these principles. Companies also should hold employees responsible for adhering to these principles. To achieve this end, companies should train their employees as appropriate to handle personal data consistently with these principles and regularly evaluate their performance in this regard. Where appropriate, companies should conduct full audits. Companies that disclose personal data to third parties should at a minimum ensure that the

recipients are under enforceable contractual obligations to adhere to these principles, unless they are required by law to do otherwise.<sup>29</sup>

The Administration's consumer privacy bill of rights legislation failed in Congress in 2012, but was revived and circulated again in 2015 as a "discussion draft". The White House ultimately halted its efforts to have the bill introduced after key public and private stakeholders criticized the bill as not going far enough or as lacking clarity.<sup>30</sup> A copy of the discussion draft is provided at Appendix A.

[go to next page]

---

<sup>29</sup> "Consumer Data Privacy in the Internet World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy", The White House, February 2012, Appendix A, pp. 47-48.

<sup>30</sup> Dana B. Rosenfeld and Alysa Zeltzer Hutnik, "Obama Administration Receives Little Support for the Consumer Privacy Bill of Rights Act", AD Law Access Blog sponsored by Kelley Drye & Warren LLP, posted in the Privacy and Information Security section. Accessed in January 2016 online at <http://www.adlawaccess.com/2015/03/articles/obama-administration-receives-little-support-for-the-consumer-privacy-bill-of-rights-act/>.

---

## **PART 3 - OPTIONS FOR FURTHER STUDY**

---

### **Organization**

A series of tables provided on the following pages compare principles distilled from the models summarized in Part 2 of this report with current provisions in the EU-U.S. Safe Harbor directive, federal law, and Montana law.

Some of the main provisions in federal and Montana laws were summarized for the committee in a previous staff paper.<sup>31</sup>

Because current law in Montana is organized by sector, the tables in this part are also organized by sector as follows:

Table 1 - Trade Practices and Consumer Protection

Table 2 - Financial & Insurance Information

Table 3 - Health Information

Table 4 - Government Information

### **Options for Committee Action**

Under the Montana law column in each table, options are offered on each principle for SAVA's consideration and possible action to help focus further study.

---

<sup>31</sup> Sheri Scurr, "HJR 21 Study of Personal Information Ownership: Overview of Current Federal & Montana Law," prepared for the State Administration and Veterans' Affairs Interim Committee, Montana Legislative Services Division, November 2013. Available online at <http://leg.mt.gov/content/Committees/Interim/2015-2016/State-Administration-and-Veterans-Affairs/Meetings/Nov-2015/HJR%2021-%20Fed%20and%20State%20Laws%20Overview.pdf>.

**Table 1 - Trade Practices and Consumer Protection**

Principle	Safe Harbor Provisions	U.S. Federal Law	Montana Law
<p><b>1. Control; Choice; Affirmative Consent (Opt-in); Right to Exit</b></p> <p><b>"Do Not Track" option for consumers would also fit under this principle.</b></p>	<p>Under the Safe Harbor principles, individuals must have a choice to opt out of the collection and forward transfer of the data to third parties.</p> <p>Opt-in is not required.</p> <p>* U.S. companies doing business that involves the collection, use and distribution of personal information about an EU resident may voluntarily certify compliance with the EU directive that articulated the Safe Harbor principles. A company that self-certifies to the FTC compliance is considered by the EU as within the Safe Harbor framework and so may do business in the EU, but may be prosecuted by the FTC for noncompliance.</p> <p>NOTE: See the update on page 9 of this report about the current status of the Safe Harbor EU-U.S. agreement.</p>	<p>Federal law does not require an opt-in choice or consent for the collection, use, or distribution of personal information.</p> <p>However, the FTC encourages businesses to voluntarily publish privacy and use policies and allow consumers to opt-out. If a company promises to provide a certain level of control or choice or gives a consumer reason to believe they have certain choices and control, and then the company fails to abide by its promises, it may be prosecuted under federal consumer protection laws as having engaged in a deceptive practice.</p>	<p>Montana's law generally follows federal fair trade and consumer protection laws. Montana Unfair Trade Practices and Consumer Protection Act of 1973 - <a href="#">Title 30, ch. 14, part 1, MCA.</a></p> <p><b><u>OPTIONS - SAVA could:</u></b></p> <ol style="list-style-type: none"> <li>1. identify specific research questions regarding certain types of information or activities, such as internet shopping, social media, cell phone tracking, etc.;</li> <li>2. examine whether to codify the Safe Harbor standard in MT laws;</li> <li>3. examine how Montana could encourage businesses to voluntarily adopt policies related to this principle and examine other state laws that may take this approach;</li> <li>4. examine amending MT law to provide more individual control than provided under the Safe Harbor standards and/or federal law and examine any other state laws that take this approach;</li> <li>5. take no further action; or</li> <li>6. take some other action?</li> </ol>

**Table 1 - Trade Practices and Consumer Protection**

Principle	Safe Harbor Provisions	U.S. Federal Law	Montana Law
<p><b>2. Transparency; Notice; Access</b></p>	<p>Individuals must be informed about what information is collected and how it will be used.</p> <p>Individuals must be able to access information held about them.</p>	<p>The FTC encourages businesses to be transparent about how they collect and use personal information by adopting privacy and use policies that the consumer has easy access to and that are understandable.</p> <p>If a company does adopt such policies, failure to follow them may be prosecuted as a deceptive practice.</p> <p>The FTC may also bring an action against a company that uses big data analytics in an unfair way that can be used to unfairly deny someone credit, housing, or access to other benefits. Thus, it encourages companies to verify that the information they are using is accurate, nondiscriminatory, and will not be used by downstream users in an unfair or deceptive way.</p>	<p>Montana's law generally mimics the federal fair trade and consumer protection laws. See Montana Unfair Trade Practices and Consumer Protection Act of 1973 - <a href="#">Title 30, ch. 14, part 1, MCA.</a></p> <p><b>OPTIONS - SAVA could:</b></p> <ol style="list-style-type: none"> <li>1. identify specific research questions regarding certain types of information or activities, such as internet shopping, social media, cell phone tracking, etc.;</li> <li>2. examine whether to codify the Safe Harbor standard in MT laws;</li> <li>3. examine how Montana could double down on the FTC's current approach to encourage voluntary compliance with this principle and examine other state laws that take this approach;</li> <li>4. examine making Montana law more restrictive than Safe Harbor or federal law and examine other state laws that may take this approach;</li> <li>5. take no further action with respect to this principle; or</li> <li>6. take some other action?</li> </ol>

**Table 1 - Trade Practices and Consumer Protection**

Principle	Safe Harbor Provisions	U.S. Federal Law	Montana Law
<p><b>3. Onward Transfer; Consistent Context (i.e, downstream use of information should be kept within purpose for which it was originally collected)</b></p>	<p>Personal information may only be transferred to third parties that follow the seven principles outlined in the Safe Harbor Directive.</p> <p>Data collected and transferred must be relevant and reliable and used only for the purpose it was collected for.</p>	<p>The FTC encourages companies to verify that the information and data they are transferring is accurate and was not obtained unfairly or fraudulently and to verify that the companies to which they are transferring the information will not use in information in an unfair or deceptive way.</p>	<p>Montana's law generally mimics the federal fair trade and consumer protection laws. See Montana Unfair Trade Practices and Consumer Protection Act of 1973 - <a href="#">Title 30, ch. 14, part 1, MCA.</a></p> <p><b>OPTIONS - SAVA could:</b></p> <ol style="list-style-type: none"> <li>1. identify specific research questions regarding certain types of information or activities, such as internet shopping, social media, cell phone tracking, etc.;</li> <li>2. examine whether to codify the Safe Harbor standard in MT laws;</li> <li>3. examine how Montana could double down on the FTC's current approach to encourage voluntary compliance with this principle and examine other state laws that may take this approach;</li> <li>4. examine making the Montana law more restrictive than federal law and examine other state laws that may take this approach;</li> <li>5. take no further action with respect to this principle; or</li> <li>6. take some other action.</li> </ol>

**Table 1 - Trade Practices and Consumer Protection**

Principle	Safe Harbor Provisions	U.S. Federal Law	Montana Law
<p><b>4. Security</b></p>	<p>To be granted "safe harbor" to do business with the EU, a company must verify to the FTC that reasonable efforts have been made to secure the information and prevent data breaches.</p>	<p><u>Section 5 of the Identify Theft Assumption and Deterrence Act of 1998, Pub. L. No. 105-318, 112 Stat. 3007, makes the FTC a central clearinghouse for identity theft complaints. The act requires the FTC to log and acknowledge such complaints, provide victims with relevant information, and refer their complaints to appropriate entities (e.g., the major national consumer reporting agencies and other law enforcement agencies).</u><sup>32</sup></p> <p><u>Personal Data Protection and Breach Accountability Act of 2014 (S.1995 - 113th Congress) 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.</u></p>	<p>Montana's laws are similar to the federal laws <a href="#">Title 30, Chapter 14, Part 17, Impediment of Identity Theft.</a></p> <p><a href="#">Section 30-14-1704, MCA</a> requires that businesses with computerized data containing personal information disclose a security breach to any resident whose "unencrypted personal information" was or is reasonably believed to have been acquired by an unauthorized person. An electronic copy must be provided to the Office of Consumer Protection.</p> <p><b><u>OPTIONS - SAVA could:</u></b></p> <ol style="list-style-type: none"> <li>1. identify specific research questions regarding certain types of information or activities, such as internet shopping, social media, cell phone tracking, etc.;</li> <li>2. further examine the Montana laws in <a href="#">T. 30, Ch. 14, Pt. 17</a> regarding security against identity theft;</li> <li>3. take no further action to examine laws related to this principle; or</li> <li>4. take some other action regarding this principle?</li> </ol>

<sup>32</sup> FTC Web site at <https://www.ftc.gov/enforcement/statutes/identity-theft-assumption-deterrence-act-1998>, January 18, 2016.

**Table 1 - Trade Practices and Consumer Protection**

Principle	Safe Harbor Provisions	U.S. Federal Law	Montana Law
<p><b>5. Data integrity; Verifiability; Right of consumer to correct or delete information</b></p>	<p>Individuals must be able to correct or delete their personal information.</p>	<p>The FTC may bring an action against a company that uses personal information, including big data analytics, in a way that differs from what it told consumers it would be used for.</p> <p>The FTC encourages companies to verify that the information and data they are collecting and/or transferring is accurate and won't be used for an unfair or fraudulent purpose.</p>	<p>Montana's law generally mimics the federal fair trade and consumer protection laws. See Montana Unfair Trade Practices and Consumer Protection Act of 1973 - <a href="#">Title 30, ch. 14, part 1, MCA.</a></p> <p><b>OPTIONS - SAVA could:</b></p> <ol style="list-style-type: none"> <li>1. identify specific research questions regarding certain types of information or activities, such as internet shopping, social media, cell phone tracking, etc.;</li> <li>2. examine whether to codify the Safe Harbor standard in MT laws;</li> <li>3. examine how Montana could double down on the FTC's current approach to encourage voluntary compliance with this principle and examine other state laws that may take this approach;</li> <li>4. examine whether Montana law should require higher standards for data integrity and examine other state laws that may take this approach;</li> <li>5. take no further action with respect to this principle; or</li> <li>6. take some other action regarding this principle?</li> </ol>



**Table 1 - Trade Practices and Consumer Protection**

Principle	Safe Harbor Provisions	U.S. Federal Law	Montana Law
<p><b>6. Accountability; Enforcement</b></p>	<p>There must be an effective means of enforcing the rules implementing the Safe Harbor principles.</p> <p>A U.S. company wishing to do business in the EU must self-certify with the FTC the company's compliance.</p>	<p>Various federal agencies have certain enforcement powers with respect to U.S. laws regarding consumer protection. See staff reported entitled "<a href="#">HJR 21 Study of Personal Information Ownership: Current Federal &amp; Montana Law</a>", November 17, 2015.</p>	<p>The Office of Consumer Protection in the Department of Justice currently fields consumer protection complaints from Montana residents. A consumer may bring a lawsuit in a district court for unfair or deceptive practices. The state Dept. of Justice may bring an action in the name of the state. County attorneys must lend support to the state Dept. of Justice and may prosecute in the name of the state.</p> <p><b><u>OPTIONS - SAVA could:</u></b></p> <ol style="list-style-type: none"> <li>1. examine Montana's current Office of Consumer Protection under the Department of Justice and identify ways to enhance its enforcement function;</li> <li>2. take no further action with respect to this principle; or</li> <li>3. take some other action regarding this principle?</li> </ol>

**Table 1 - Trade Practices and Consumer Protection**

<b>Principle</b>	<b>Safe Harbor Provisions</b>	<b>U.S. Federal Law</b>	<b>Montana Law</b>
<p><b>7. Other Issues</b> - Do SAVA members have any other research questions or policy concerns regarding consumer information? For example: Social media privacy (See NCSL articles)?</p>			

## Note About Table 2

Table 2 relates to financial and insurance information. Generally, the EU-U.S. Safe Harbor agreement does not apply to financial and insurance companies.

The U.S. Department of Commerce publishes the following statement on its Web page regarding Safe Harbor principles and the financial sector:

Only U.S. organizations subject to the jurisdiction of the Federal Trade Commission (FTC) or U.S. air carriers and ticket agents subject to the jurisdiction of the Department of Transportation (DOT) may participate in the Safe Harbor. Organizations generally not subject to FTC jurisdiction include certain **financial institutions, (such as banks, investment houses, credit unions, and savings & loan institutions)**, telecommunication common carriers, labor associations, non-profit organizations, agricultural co-operatives, and meat processing facilities. In addition, the FTC's jurisdiction with regard to insurance activities is limited to certain circumstances. If you are uncertain as to whether your organization falls under the jurisdiction of either the FTC or DOT, as certain exceptions to general ineligibility do exist, be sure to contact those agencies for more information.<sup>33</sup>

Table 2 compares only federal and Montana laws to the model principles. Research on other international agreements concerning personal information that may apply to financial institutions was not conducted for this paper.

---

<sup>33</sup> See <http://www.export.gov/safeharbor/>.

**Table 2 - Financial & Insurance Information**

Principle	Federal Law	Montana Law	Options
<p><b>1. Control; Choice; Affirmative Consent (Opt-in); Right to Exit</b></p>	<p><u>Gramm-Leach-Bliley Act:</u> Covered financial institutions covered by the must provide customers the right to "opt out" if they don't want their information shared with certain third parties. <a href="#">FTC Web Site on How to Comply with GLB</a></p> <p><u>Fair Credit Reporting Act</u> (15 U.S.C. 1681, et. seq.): - customers must consent before the credit report is given to an employer; - customers must be able to opt out when they are sent unsolicited "prescreening/prequalification" offers.</p> <p>See November HJR 21 <a href="#">staff report</a> on federal and state laws.</p> <p><u>Public Law 79-15</u> <u>(the McCarran-Ferguson Act,</u> <u>15 U.S.C. 1011 through 1015)</u> March 9, 1945 * this law was not reviewed for this report</p>	<p><u>Consumer Protection Act</u> - <a href="#">Title 30, ch. 14, pt. 1, MCA</a></p> <p><u>Insurance and Insurance Companies- Unfair or Deceptive Trade Practices by Insurers:</u> - <a href="#">Title 33, ch. 18, MCA</a></p> <p><u>Insurance Information and Privacy Protection Act</u> - <a href="#">Title 33, ch. 19, MCA</a></p> <p>See November HJR 21 <a href="#">staff report</a> on federal and state laws.</p> <p>Consent is required before personal or privileged information may be disclosed, but personal information may be disclosed for marketing purposes based on certain conditions.</p> <p>(See Principle 3 summary)</p>	<p><b><u>SAVA could:</u></b></p> <ol style="list-style-type: none"> <li>1. further examine federal and Montana laws on financial and insurance information with respect to this principle;</li> <li>2. take no further action with respect to this principle; or</li> <li>3. take some other action regarding this principle?</li> </ol>

**Table 2 - Financial & Insurance Information**

Principle	Federal Law	Montana Law	Options
<p><b>2. Transparency; Notice; Access</b></p>	<p><u>Gramm-Leach-Bliley Act:</u> Covered entities must tell their customers about their information-sharing practices.</p> <p><u>Fair Credit Reporting Act</u> (15 U.S.C. 1681, et. seq.): Customers have the right to:</p> <ul style="list-style-type: none"> <li>- know what it is their credit reports;</li> <li>- be notified if information in their credit reports has been used to deny an application.</li> </ul>	<p><u>Insurance Information and Privacy Protection Act - Title 33, ch. 19, MCA</u> - examples below:</p> <p><a href="#">33-19-202</a> - Customers must receive "clear and conspicuous" notice of information practices. Questions designed to gather personal information solely for marketing or research must be clearly specified.</p> <p><a href="#">33-19-203</a> - Disclosure of information that is requested solely for marketing or research purposes.</p> <p><a href="#">33-19-205</a> - Disclosures concerning investigative consumer reports.</p> <p><a href="#">33-19-301</a> - Access to recorded personal information</p> <ul style="list-style-type: none"> <li>- specifies how a person may request access to their personal information and how long an insurance institution has to respond.</li> <li>- specifies what information must be accessible.</li> <li>- allows individual to request to know who has been given the person's personal information.</li> </ul> <p>Customers may request:</p> <ul style="list-style-type: none"> <li>- a copy of investigative consumer reports.</li> <li>- access to recorded personal information.</li> <li>- information specifying the reasons for an adverse underwriting decision</li> </ul>	<p><b><u>SAVA could:</u></b></p> <ol style="list-style-type: none"> <li>1. further examine federal and Montana laws on financial and insurance information with respect to this principle;</li> <li>2. take no further action with respect to this principle; or</li> <li>3. take some other action regarding this principle?</li> </ol>

**Table 2 - Financial & Insurance Information**

Principle	Federal Law	Montana Law	Options
<p><b>3. Onward Transfer; Consistent Context (i.e, downstream use of information should be kept within purpose for which it was originally collected)</b></p>	<p><u>Gramm-Leach-Bliley Act:</u> Customers must:</p> <ul style="list-style-type: none"> <li>- have the opportunity to direct that personal information not be disclosed to unaffiliated third parties; and</li> <li>- receive an explanation of how to exercise that nondisclosure option.</li> </ul> <p><u>Exception:</u> 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:</p> <ul style="list-style-type: none"> <li>-marketing the financial institution's own products or services; or</li> <li>- marketing financial products or services offered pursuant to joint agreements between two or more financial institutions that comply with certain requirements, if:               <ul style="list-style-type: none"> <li>- the financial institution fully discloses to the customer that it is providing the information; and</li> <li>- the financial institution enters into a contractual agreement with the third party that requires the third party to maintain the confidentiality of the information.</li> </ul> </li> </ul>	<p><u>Insurance Information and Privacy Protection Act - Title 33, ch. 19, MCA</u> - examples below: See <a href="#">Section 33-19-306, MCA</a> - disclosure limitations and conditions See <a href="#">Section 33-19-307, MCA</a> - marketing Licensee may not use or disclose personal information for marketing reasons, <b>except:</b> licensee may use or disclose to another licensee personal information for marketing purposes "if reasonably necessary" to:</p> <ul style="list-style-type: none"> <li>- market insurance or financial products or services;</li> <li>- enable an affiliate to market insurance or financial products and services;</li> <li>- enable a person contractually engaged to provide services for or on behalf of the licensee to market insurance or financial products and services.</li> </ul> <p>Any other use or disclosure requires the individual's written consent. The authorization must:</p> <ul style="list-style-type: none"> <li>- be clear and conspicuous disclosure about marketing purpose;</li> <li>- specify each entity or type of entity to which information would be disclosed;</li> <li>- specify what information would be disclosed; and</li> <li>- specify type of marketing individual might receive.</li> </ul> <p>See also Montana Mortgage Act <a href="#">32-9-160</a> - confidentiality</p>	<p><b><u>SAVA could:</u></b></p> <ol style="list-style-type: none"> <li>1. further examine federal and Montana laws on financial and insurance information with respect to this principle;</li> <li>2. take no further action with respect to this principle; or</li> <li>3. take some other action regarding this principle?</li> </ol>

**Table 2 - Financial & Insurance Information**

Principle	Federal Law	Montana Law	Options
<p><b>4. Security</b></p>	<p><u>Personal Data Protection and Breach Accountability Act of 2014 (S.1995 - 113th Congress)</u></p> <p>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.</p>	<p><u>Insurance Information and Privacy Protection Act</u>                      - <a href="#">Title 33, ch. 19, MCA</a></p> <p><a href="#">33-19-321</a> - Individuals have the right to notice of any security breach that has resulted in the disclosure of unencrypted personal information.</p> <p>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:</p> <ul style="list-style-type: none"> <li>- social security number;</li> <li>- driver's license, state, or tribal id number;</li> <li>- an account number;</li> <li>- medical record information;</li> <li>- taxpayer id number; or</li> <li>- an identity protection personal id number issued by the IRS.</li> </ul> <p><u>Impediment to Identity Theft</u>                      - <a href="#">Title 30, ch. 14, part 17, MCA</a></p>	<p><b><u>SAVA could:</u></b></p> <ol style="list-style-type: none"> <li>1. further examine federal and Montana laws on financial and insurance information with respect to this principle;</li> <li>2. take no further action with respect to this principle; or</li> <li>3. take some other action regarding this principle?</li> </ol>

**Table 2 - Financial & Insurance Information**

Principle	Federal Law	Montana Law	Options
<p><b>5. Data integrity; Verifiability; Right of consumer to correct or delete information</b></p>	<p><u>Gramm-Leach-Bliley Act</u> 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.):</p> <ul style="list-style-type: none"> <li>- Bureau of Consumer Financial Protection (created by the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010);</li> <li>- Federal Trade Commission;</li> <li>- federal functional regulators; and</li> <li>- state insurance authorities.</li> </ul> <p><u>Fair Credit Reporting Act</u> Customers have the right to:</p> <ul style="list-style-type: none"> <li>- dispute incomplete, inaccurate, outdated information; and</li> <li>- require information that a credit reporting agency cannot verify be removed or corrected.</li> </ul>	<p><u>Insurance Information and Privacy Protection Act</u> - Title 33, ch. 19, MCA</p> <p>Individuals may request corrections, amendments, or deletions of recorded personal information.</p>	<p><b><u>SAVA could:</u></b></p> <ol style="list-style-type: none"> <li>1. further examine federal and Montana laws on financial and insurance information with respect to this principle;</li> <li>2. take no further action with respect to this principle; or</li> <li>3. take some other action regarding this principle?</li> </ol>



**Table 2 - Financial & Insurance Information**

Principle	Federal Law	Montana Law	Options
<p><b>6. Accountability; Enforcement</b></p>	<p><u>Fair Credit Reporting Act</u></p> <ul style="list-style-type: none"> <li>- Individuals have a private right of action and may file civil lawsuits in federal or state courts.</li> <li>- Fraud and other knowing and willful violations may result in criminal prosecution.</li> <li>- Federal enforcement agencies that may regulate and handle complaints include:                             <ul style="list-style-type: none"> <li>o FTC;</li> <li>o Department of the Treasury;</li> <li>o Federal Reserve;</li> <li>o National Credit Union Admin o Federal Deposit Insurance Corp ;</li> <li>o Department of Transportation;</li> <li>o Department of Agriculture.</li> </ul> </li> </ul>	<p><u>Impediment to Identify Theft</u></p> <ul style="list-style-type: none"> <li>- Title 30, ch. 14, part 1, MCA</li> </ul> <p>Montana state enforcement agencies include:</p> <ul style="list-style-type: none"> <li>- Office of Consumer Protection, Department of Justice;</li> <li>- State Auditor's Office; and</li> <li>- Banking and Financial Institutions Division, Department of Administration.</li> </ul> <p><u>Insurance Information and Privacy Protection Act</u></p> <ul style="list-style-type: none"> <li>- Title 33, ch. 19, MCA</li> </ul> <p>Montana's Commission of Insurance (i.e., the State Auditor's Office) is empowered to</p> <ul style="list-style-type: none"> <li>- examine and investigate covered entities; and</li> <li>- impose fines.</li> </ul> <p>Harmed individuals have a private right of action (i.e., may file a civil lawsuit).</p> <p>The Attorney General or a county attorney may prosecute for criminal violations.</p>	<p><b><u>SAVA could:</u></b></p> <ol style="list-style-type: none"> <li>1. further examine federal and Montana laws on financial and insurance information with respect to this principle;</li> <li>2. take no further action with respect to this principle; or</li> <li>3. take some other action regarding this principle?</li> </ol>

**Table 2 - Financial & Insurance Information**

<b>Principle</b>	<b>Federal Law</b>	<b>Montana Law</b>	<b>Options</b>
------------------	--------------------	--------------------	----------------

**7. Other Issues** - Do SAVA members have any other research questions or policy concerns regarding financial and insurance information?

**Table 3 - Health Information**

Principle	Federal Law	Montana Law	Options
<p><b>1. Control; Choice; Affirmative Consent (Opt-in); Right to Exit</b></p>	<p><u>Health Insurance Portability and Accountability Act (HIPAA)</u> - Pub. L. 104-191</p> <p>Patients must consent to the use or sharing of their health information for certain purposes, such as for marketing.</p>	<p><u>Uniform Health Care Information Act</u> - Title 50, Ch. 16</p> <p><a href="#">Part 5 - Uniform Health Care Info.</a> - applies only to health care providers <b>not</b> covered by HIPAA - affirmative consent required, with exceptions - patient may revoke consent</p>	<p><b>SAVA could:</b></p> <ol style="list-style-type: none"> <li>1. further examine whether Montana law should give individuals more control and choice than HIPAA (be as specific as possible);</li> <li>2. further examine Montana law to ensure match with HIPAA for the non-HIPAA entities;</li> <li>3. take no further action with respect to this principle; or</li> <li>4. take some other action regarding this principle</li> </ol>
<p><b>2. Transparency; Notice; Access</b></p>	<p><u>Health Insurance Portability and Accountability Act (HIPAA)</u> - Pub. L. 104-191</p> <p>Patients have the right to:</p> <ul style="list-style-type: none"> <li>- receive a notice about how their health information may be used and shared;</li> <li>- ask to see and get a copy of their health records</li> </ul>	<p><u>Uniform Health Care Information Act</u> - Title 50, Ch. 16</p> <p><a href="#">Part 5 - Uniform Health Care Info.</a> - notice of information required, form prescribed in 50-16-512 - patients may examine and copy their health information.</p>	<p><b>SAVA could:</b></p> <ol style="list-style-type: none"> <li>1. further examine whether Montana law should provide more transparency, notice, and access than HIPAA (be as specific as possible);</li> <li>2. further examine Montana law to ensure match with HIPAA for the non-HIPAA entities;</li> <li>3. take no further action with respect to this principle; or</li> <li>4. take some other action regarding this principle</li> </ol>

**Table 3 - Health Information**

Principle	Federal Law	Montana Law	Options
<p><b>3. Onward Transfer; Consistent Context (i.e, downstream use of information should be kept within purpose for which it was originally collected)</b></p>	<p>Health Insurance Portability and Accountability Act (HIPAA) - Pub. L. 104-191</p> <p>Patients have the right to:</p> <ul style="list-style-type: none"> <li>- obtain a report on when and why their health information was shared for certain purposes;</li> </ul> <p>The law allows health information to be used and shared for the following reasons:</p> <ul style="list-style-type: none"> <li>- treatment and care coordination;</li> <li>- payment for services;</li> <li>- with family, relatives, friends, or others identified by patients as involved with their health care or responsible for payment;</li> <li>- for quality control;</li> <li>- to protect the public's health; and</li> <li>- to make required reports to law enforcement or as ordered by a court.</li> </ul>	<p><u>Uniform Health Care Information Act</u> - Title 50, Ch. 16</p> <p><u>Part 8 - Privacy Requirements</u> - applies only to health care providers that are subject to HIPAA</p> <p>- more stringent than HIPAA in some cases, but less stringent than California</p> <p>- Erin MacLean stated that <u>50-16-812</u> - concerns when information is subject to compulsory disclosure process - violates HIPAA and needs to be fixed</p> <p>- Erin MacLean also stated that the "business associates" who may receive personal medical information without affirmative consent and/or disclosure is not clear in current law</p>	<p><b>SA</b></p> <ol style="list-style-type: none"> <li>1. further examine whether [redacted] specific as possible);</li> <li>2. further examine Montana law to ensure match with HIPAA for the non-HIPAA entities;</li> <li>3. examine 50-16-812, MCA, and consider amendments so it does not violate HIPAA;</li> <li>4. examine the business associates issue raised by Ms. MacLean;</li> <li>5. take no further action with respect to this principle; or</li> <li>6. take some other action regarding this principle</li> </ol>

**Table 3 - Health Information**

Principle	Federal Law	Montana Law	Options
<p><b>4. Security</b></p>	<p><u>HITECH Act</u>                      - this law provides greater emphasis on security, adds to HIPAA and other data security laws                      - patients must be notified of any security breach.                      - if a breach impacts 500 patients or more, then HHS must also be notified. Notification will trigger posting the breaching entity's name on HHS' website.                      - under certain conditions local media must also be notified.                      - notification is triggered whether the breach occurred externally or internally.</p>	<p><u>Unfair Trade Practices</u>  <a href="#">Section 30-14-1704, MCA.</a></p> <p><u>Insurance Companies</u>  <a href="#">Section 33-19-321, MCA.</a></p> <p>- individuals must be notified of a security breach compromising their "medical record information"                      - consumer protection office under Dept. of Justice must also be notified</p>	<p><b>SAVA could:</b></p> <ol style="list-style-type: none"> <li>1. further examine whether Montana law could better reflect the HITECH Act with respect to those entities not covered by HIPAA);</li> <li>2. further examine Montana law to ensure match with HIPAA for the non-HIPAA entities;</li> <li>3. take no further action with respect to this principle; or</li> <li>4. take some other action regarding this principle</li> </ol>
<p><b>5. Data integrity; Verifiability; Right of consumer to correct or delete information</b></p>	<p><u>Health Insurance Portability and Accountability Act (HIPAA)</u>                      - Pub. L. 104-191</p> <p>- patients have the right to correct their health information.</p>	<p><u>Uniform Health Care Information Act</u>                      - Title 50, Ch. 16</p> <p>- patients may submit corrections to their health information.</p>	<p><b>SAVA could:</b></p> <ol style="list-style-type: none"> <li>1. further examine whether Montana law should be stricter than HIPAA;</li> <li>2. further examine Montana law to ensure match with HIPAA for the non-HIPAA entities;</li> <li>3. take no further action with respect to this principle; or</li> <li>4. take some other action regarding this principle</li> </ol>

**Table 3 - Health Information**

Principle	Federal Law	Montana Law	
<p><b>6. Accountability; Enforcement</b></p>	<p><u>Health Insurance Portability and Accountability Act (HIPAA)</u> - Pub. L. 104-191</p> <p>Patients may: - file a complaint with a provider or health insurer if they believe their health information was not kept confidential; or - file a complaint with HHS</p> <p><u>HITECH Act</u> - mandatory penalties for "willful neglect." - penalties were increased</p> <p>See Page 17 of Nov. 17 Staff Report</p>	<p><u>Uniform Health Care Information Act</u> - Title 50, Ch. 16</p> <p>Criminal and civil penalties are provided for in statute and the state attorney general or a county attorney is authorized to prosecute violations.</p> <p>Erin MacLean testified: - there isn't any policing and no state-level agency to field complaints</p> <p>- the penalties and fines in state statutes do not track with the federal penalties</p> <p>- CA could be a state to examine for stronger accountability and enforcement</p>	<p><b>SAVA could:</b></p> <ol style="list-style-type: none"> <li>1. further examine whether Montana law should be stricter than HIPAA;</li> <li>2. further examine Montana law to ensure match with HIPAA for the non-HIPAA entities;</li> <li>3. consider state-level policing</li> <li>4. consider state penalties matching the HIPAA and HITECH penalties</li> <li>5. take no further action with respect to this principle; or</li> <li>6. take some other action regarding this principle</li> </ol>

**7. Other Issues** - Do SAVA members have any other research questions or policy concerns regarding this type of information?

**Table 4 - Government Information**

Principle	Federal Law	Montana Law	Options
<p><b>1. Control; Choice; Affirmative Consent (Opt-in); Right to Exit</b></p>	<p><u>Privacy Act of 1974 - 5 U.S.C. 552 et. seq.</u>                      “No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains...” [subject to 12 exceptions].</p> <p><u>E-Government Act of 2002</u></p>	<p><u>State Agency Protection of Personal Information</u>                      - <a href="#">Title 2, ch. 6, part 15, MCA</a></p> <p>See pages 23-24 in Nov. 17 staff report.</p> <p><u>Montana Information Technology Act</u>                      - <a href="#">Title 2, ch. 17, part 5</a>                      - affirmative consent is required before a government website may collect personally identifiable information that will be passed on to a third party</p>	<p><b>SAVA could:</b></p> <ol style="list-style-type: none"> <li>1. further examine federal law and compare it with Montana law</li> <li>2. further examine Montana law</li> <li>3. take no further action</li> <li>4. take some other action</li> </ol>
<p><b>2. Transparency; Notice; Access</b></p>		<p><u>Montana Information Technology Act</u>                      - <a href="#">Title 2, ch. 17, part 5</a>  <a href="#">2-17-552</a> - government website                      - must generally describe information practices and operator's policies to protect privacy</p>	<p><b>SAVA could:</b></p> <ol style="list-style-type: none"> <li>1. further examine federal law and compare it with Montana law</li> <li>2. further examine Montana law</li> <li>3. take no further action</li> <li>4. take some other action</li> </ol>

**Table 4 - Government Information**

Principle	Federal Law	Montana Law	Options
<p><b>3. Onward Transfer; Consistent Context (i.e, downstream use of information should be kept within purpose for which it was originally collected)</b></p>		<p><u>Montana Information Technology Act - Title 2, ch. 17, part 5</u></p> <p><u>2-17-552</u> - government website                      - if personally identifiable information is to be used for a purpose other than for the purposes of the website, operator must provide "clear and conspicuous notice", provide a general description of the types of third parties may obtain the information, and require the affirmative expression of the user's permission before the information is collected</p>	<p><b>SAVA could:</b></p> <ol style="list-style-type: none"> <li>1. further examine federal law and compare it with Montana law</li> <li>2. further examine Montana law</li> <li>3. take no further action</li> <li>4. take some other action</li> </ol>
<p><b>4. Security</b></p>		<p><u>Montana Information Technology Act - Title 2, ch. 17, part 5</u></p> <p><u>2-17-534</u> - Dept. of Administration (Chief Information Officer) - must develop guidelines and training for state agencies</p>	<p><b>SAVA could:</b></p> <ol style="list-style-type: none"> <li>1. further examine federal law and compare it with Montana law</li> <li>2. further examine Montana law</li> <li>3. take no further action</li> <li>4. take some other action</li> </ol>



**Table 4 - Government Information**

Principle	Federal Law	Montana Law	Options
<p><b>5. Data integrity; Verifiability; Right of consumer to correct or delete information</b></p>		<p>Not addressed</p>	<p><b><u>SAVA could:</u></b></p> <ol style="list-style-type: none"> <li>1. further examine federal law and compare it with Montana law</li> <li>2. further examine Montana law</li> <li>3. take no further action</li> <li>4. take some other action</li> </ol>
<p><b>6. Accountability; Enforcement</b></p>		<p><a href="#">2-17-514</a> - "If the department determines that an agency is not in compliance with the state strategic information technology plan provided for in 2-17-521, the agency information technology plan provided for in 2-17-523, or the statewide information technology policies and standards provided for in 2-17-512, the department may cancel or modify any contract, project, or activity that is not in compliance."</p>	<p><b><u>SAVA could:</u></b></p> <ol style="list-style-type: none"> <li>1. further examine federal law and compare it with Montana law</li> <li>2. further examine Montana law</li> <li>3. take no further action</li> <li>4. take some other action</li> </ol>

## Table 4 - Government Information

Principle	Federal Law	Montana Law	Options
<p><b>7. Other Issues</b> - Do SAVA members have any other research questions or policy concerns regarding this type of information?</p> <ul style="list-style-type: none"><li>a. <u>Uniform Health Care Information Act</u> - Title 50, Ch. 16 <a href="#">Part 6 - Government Health Care Info.</a><ul style="list-style-type: none"><li>- government entities with health care information must still comply with HIPAA</li><li>- Erin MacLean testified that the need to also comply with HIPAA should be clarified in the Part 6 statutes.</li></ul></li><li>b. Law enforcement information (for example, mug shots on websites; arrest records, indictments or other legal or court documents if there has been an acquittal or no charges filed, etc.)?</li><li>c. Others?</li></ul>			