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."[1]

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.

[1] 64th Montana Legislature, House Joint Resolution 21, subsection (2), 2015.

However, a review of literature and legal analysis in this are 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 through 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.[2]

[2] 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."[3]

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.[4]

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.[5]

---

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

[4] 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/ ISSN: 2278-5612.

[5] 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.[6]

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.[7]

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.[8]

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.

---

[6] Paul M. Schwartz, "Property, Privacy, and Personal Data", 117 *Harvard Law Review* 2056, 2003-2004.

[7] Al-Khouri, p.4.

[8] 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.[9]

Some ownership is inalienable

Schwartz describes the levels of ownership a bit differently than Al-Khouri. 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, Schwatrz 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.[10]

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.[11]

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

[9] Al-Khouri, p. 3.

[10] Schwartz, p. 2097.

[11] 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".[12]

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.[13]

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.[14]

---

[12] Schwartz, p. 2058.

[13] 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.

[14] 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."[15]

[go to next page]

[15] 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.[16]

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.[17]

Safe Harbor Model - An International Agreement

Background

In 1995, the European Union adopted a directive (updated by a European Commission decision in 2001)[18] 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.[19]

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

[16] 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.

[17] 64th Montana Legislature, HJR 21 (2015).

[18] 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.

[19] Wikipedia, "International Safe Harbor Privacy Principles", accessed in January 2016 at 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.[20]

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." [21]

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.

[20] 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.

[21] European Commission Web site under the data protection topic at 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.[22]

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.[23]

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

[23] Schwartz, p. 2094.

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

1. **Opt-in requirement** - For companies to a 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."[24]

The table on the following page is taken directly from Al-Khouri's article.[25]

[24] Al-Khouri, p. 1.

[25] Ibid., p. 5.

Guiding Principle	Description
Accountability	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.
Enforcement:	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.
Data permissions:	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.
Balanced stakeholder roles:	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.
Anonymity and identity:	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.
Shared data commons:	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.[26]

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.

[26] 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.[27]

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.[28]

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

[27] Ibid., pp. 3-4.

[28] "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, 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.[29]

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.[30] A copy of the discussion draft is provided at Appendix A.

[go to next page]

[29] "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.

[30] 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 pervious staff paper.[31]

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.

[31] 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**
1. Control; Choice; Affirmative Consent (Opt-in); Right to Exit **"Do Not Track" option for consumers would also fit under this principle.**	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. Opt-in is not required. * 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. NOTE: See the update on page 9 of this report about the current status of the Safe Harbor EU-U.S. agreement.	Federal law does not require an opt-in choice or consent for the collection, use, or distribution of personal information. 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.	Montana's law generally follows federal fair trade and consumer protection laws. Montana Unfair Trade Practices and Consumer Protection Act of 1973 - Title 30, ch. 14, part 1, MCA. **OPTIONS - SAVA could:** 1. identify specific research questions regarding certain types of information or activities, such as internet shopping, social media, cell phone tracking, etc.; 2. examine whether to codify the Safe Harbor standard in MT laws; 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; 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; 5. take no further action; or 6. take some other action?

Table 1 - Trade Practices and Consumer Protection			
Principle	**Safe Harbor Provisions**	**U.S. Federal Law**	**Montana Law**
2. Transparency; Notice; Access	Individuals must be informed about what information is collected and how it will be used. Individuals must be able to access information held about them.	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. If a company does adopt such policies, failure to follow them may be prosecuted as a deceptive practice. 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.	Montana's law generally mimics the federal fair trade and consumer protection laws. See Montana Unfair Trade Practices and Consumer Protection Act of 1973 - Title 30, ch. 14, part 1, MCA. **OPTIONS - SAVA could:** 1. identify specific research questions regarding certain types of information or activities, such as internet shopping, social media, cell phone tracking, etc.; 2. examine whether to codify the Safe Harbor standard in MT laws; 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; 4. examine making Montana law more restrictive than Safe Harbor or federal law and examine other state laws that may take this approach; 5. take no further action with respect to this principle; or 6. take some other action?

Table 1 - Trade Practices and Consumer Protection			
Principle	**Safe Harbor Provisions**	**U.S. Federal Law**	**Montana Law**
3. Onward Transfer; Consistent Context (i.e, downstream use of information should be kept within purpose for which it was originally collected)	Personal information may only be transferred to third parties that follow the seven principles outlined in the Safe Harbor Directive. Data collected and transferred must be relevant and reliable and used only for the purpose it was collected for.	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.	Montana's law generally mimics the federal fair trade and consumer protection laws. See Montana Unfair Trade Practices and Consumer Protection Act of 1973 - Title 30, ch. 14, part 1, MCA. **OPTIONS - SAVA could:** 1. identify specific research questions regarding certain types of information or activities, such as internet shopping, social media, cell phone tracking, etc.; 2. examine whether to codify the Safe Harbor standard in MT laws; 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; 4. examine making the Montana law more restrictive than federal law and examine other state laws that may take this approach; 5. take no further action with respect to this principle; or 6. take some other action.

Table 1 - Trade Practices and Consumer Protection			
Principle	**Safe Harbor Provisions**	**U.S. Federal Law**	**Montana Law**
4. Security	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.	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).[32] 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.	Montana's laws are similar to the federal laws Title 30, Chapter 14, Part 17, Impediment of Identity Theft. Section 30-14-1704, MCA 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. **OPTIONS - SAVA could:** 1. identify specific research questions regarding certain types of information or activities, such as internet shopping, social media, cell phone tracking, etc.; 2. further examine the Montana laws in T. 30, Ch. 14, Pt. 17 regarding security against identity theft; 3. take no further action to examine laws related to this principle; or 4. take some other action regarding this principle?

[32] 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**
5. Data integrity; Verifiability; Right of consumer to correct or delete information	Individuals must be able to correct or delete their personal information.	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. 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.	Montana's law generally mimics the federal fair trade and consumer protection laws. See Montana Unfair Trade Practices and Consumer Protection Act of 1973 - Title 30, ch. 14, part 1, MCA. **OPTIONS - SAVA could:** 1. identify specific research questions regarding certain types of information or activities, such as internet shopping, social media, cell phone tracking, etc.; 2. examine whether to codify the Safe Harbor standard in MT laws; 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; 4. examine whether Montana law should require higher standards for data integrity and examine other state laws that may take this approach; 5. take no further action with respect to this principle; or 6. take some other action regarding this principle?

Table 1 - Trade Practices and Consumer Protection			
Principle	**Safe Harbor Provisions**	**U.S. Federal Law**	**Montana Law**
6. Accountability; Enforcement	There must be an effective means of enforcing the rules implementing the Safe Harbor principles. A U.S. company wishing to do business in the EU must self-certify with the FTC the company's compliance.	Various federal agencies have certain enforcement powers with respect to U.S. laws regarding consumer protection. See staff reported entitled "HJR 21 Study of Personal Information Ownership: Current Federal & Montana Law", November 17, 2015.	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. **OPTIONS - SAVA could:** 1. examine Montana's current Office of Consumer Protection under the Department of Justice and identify ways to enhance its enforcement function; 2. take no further action with respect to this principle; or 3. take some other action regarding this principle?

Table 1 - Trade Practices and Consumer Protection			
Principle	**Safe Harbor Provisions**	**U.S. Federal Law**	**Montana Law**
7. Other Issues - Do SAVA members have any other research questions or policy concerns regarding consumer information? For example: Social media privacy (See NCSL articles)?			

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.[33]

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.

[33] See http://www.export.gov/safeharbor/.

Table 2 - Financial & Insurance Information			
Principle	**Federal Law**	**Montana Law**	**Options**
1. Control; Choice; Affirmative Consent (Opt-in); Right to Exit	Gramm-Leach-Bliley Act: 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. FTC Web Site on How to Comply with GLB Fair Credit Reporting Act (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. See November HJR 21 staff report on federal and state laws. Public Law 79-15 (the McCarran-Ferguson Act, 15 U.S.C. 1011 through 1015) March 9, 1945 * this law was not reviewed for this report	Consumer Protection Act - Title 30, ch. 14, pt. 1, MCA Insurance and Insurance Companies- Unfair or Deceptive Trade Practices by Insurers: - Title 33, ch. 18, MCA Insurance Information and Privacy Protection Act - Title 33, ch. 19, MCA See November HJR 21 staff report on federal and state laws. Consent is required before personal or privileged information may be disclosed, but personal information may be disclosed for marketing purposes based on certain conditions. (See Principle 3 summary)	**SAVA could:** 1. further examine federal and Montana laws on financial and insurance information with respect to this principle; 2. take no further action with respect to this principle; or 3. take some other action regarding this principle?

Table 2 - Financial & Insurance Information			
Principle	**Federal Law**	**Montana Law**	**Options**
2. Transparency; Notice; Access	Gramm-Leach-Bliley Act: Covered entities must tell their customers about their information-sharing practices. Fair Credit Reporting Act (15 U.S.C. 1681, et. seq.): Customers have 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.	Insurance Information and Privacy Protection Act - Title 33, ch. 19, MCA - examples below: 33-19-202 - 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. 33-19-203 - Disclosure of information that is requested solely for marketing or research purposes. 33-19-205 - Disclosures concerning investigative consumer reports. 33-19-301 - Access to recorded personal information - specifies how a person may request access to their personal information and how long an insurance institution has to respond. - specifies what information must be accessible. - allows individual to request to know who has been given the person's personal information. Customers may request: - a copy of investigative consumer reports. - access to recorded personal information. - information specifying the reasons for an adverse underwriting decision	**SAVA could:** 1. further examine federal and Montana laws on financial and insurance information with respect to this principle; 2. take no further action with respect to this principle; or 3. take some other action regarding this principle?

Table 2 - Financial & Insurance Information			
Principle	**Federal Law**	**Montana Law**	**Options**
3. Onward Transfer; Consistent Context (i.e, downstream use of information should be kept within purpose for which it was originally collected)	Gramm-Leach-Bliley Act: Customers must: - have the opportunity to direct that personal information not be disclosed to unaffiliated third parties; and - receive an explanation of how to exercise that nondisclosure option. 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.	Insurance Information and Privacy Protection Act - Title 33, ch. 19, MCA - examples below: See Section 33-19-306, MCA - disclosure limitations and conditions See Section 33-19-307, MCA - marketing Licensee may not use or disclose personal information for marketing reasons, **except**: licensee may use or disclose to another licensee personal information for marketing purposes "if reasonably necessary" to: - market insurance or financial products or services; - enable an affiliate to market insurance or financial products and services; - enable a person contractually engaged to provide services for or on behalf of the licensee to market insurance or financial products and services. Any other use or disclosure requires the individual's written consent. The authorization must: - be clear and conspicuous disclosure about marketing purpose; - specify each entity or type of entity to which information would be disclosed; - specify what information would be disclosed; and - specify type of marketing individual might receive. See also Montana Mortgage Act 32-9-160 - confidentiality	**SAVA could:** 1. further examine federal and Montana laws on financial and insurance information with respect to this principle; 2. take no further action with respect to this principle; or 3. take some other action regarding this principle?

Table 2 - Financial & Insurance Information			
Principle	**Federal Law**	**Montana Law**	**Options**
4. Security	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.	Insurance Information and Privacy Protection Act - Title 33, ch. 19, MCA 33-19-321 - Individuals have the right to 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. Impediment to Identity Theft - Title 30, ch. 14, part 17, MCA	**SAVA could:** 1. further examine federal and Montana laws on financial and insurance information with respect to this principle; 2. take no further action with respect to this principle; or 3. take some other action regarding this principle?

Table 2 - Financial & Insurance Information			
Principle	**Federal Law**	**Montana Law**	**Options**
5. Data integrity; Verifiability; Right of consumer to correct or delete information	Gramm-Leach-Bliley Act 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. Fair Credit Reporting Act Customers have the right to: - dispute incomplete, inaccurate, outdated information; and - require information that a credit reporting agency cannot verify be removed or corrected.	Insurance Information and Privacy Protection Act - Title 33, ch. 19, MCA Individuals may request corrections, amendments, or deletions of recorded personal information.	**SAVA could:** 1. further examine federal and Montana laws on financial and insurance information with respect to this principle; 2. take no further action with respect to this principle; or 3. take some other action regarding this principle?

Table 2 - Financial & Insurance Information			
Principle	**Federal Law**	**Montana Law**	**Options**
6. Accountability; Enforcement	Fair Credit Reporting Act - 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: o FTC; o Department of the Treasury; o Federal Reserve; o National Credit Union Admin o Federal Deposit Insurance Corp ; o Department of Transportation; o Department of Agriculture.	Impediment to Identify Theft - Title 30, ch. 14, part 1, MCA 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. Insurance Information and Privacy Protection Act - Title 33, ch. 19, MCA 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.	**SAVA could:** 1. further examine federal and Montana laws on financial and insurance information with respect to this principle; 2. take no further action with respect to this principle; or 3. take some other action regarding this principle?

Table 2 - Financial & Insurance Information			
Principle	**Federal Law**	**Montana Law**	**Options**
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**
1. Control; Choice; Affirmative Consent (Opt-in); Right to Exit	Health Insurance Portability and Accountability Act (HIPAA) - Pub. L. 104-191 Patients must consent to the use or sharing of their health information for certain purposes, such as for marketing.	Uniform Health Care Information Act - Title 50, Ch. 16 Part 5 - Uniform Health Care Info. - applies only to health care providers **not** covered by HIPAA - affirmative consent required, with exceptions - patient may revoke consent	**SAVA could:** 1. further examine whether Montana law should give individuals more control and choice than HIPAA (be as specific as possible); 2. further examine Montana law to ensure match with HIPAA for the non-HIPAA entities; 3. take no further action with respect to this principle; or 4. take some other action regarding this principle
2. Transparency; Notice; Access	Health Insurance Portability and Accountability Act (HIPAA) - Pub. L. 104-191 Patients have the right to: - receive a notice about how their health information may be used and shared; - ask to see and get a copy of their health records	Uniform Health Care Information Act - Title 50, Ch. 16 Part 5 - Uniform Health Care Info. - notice of information required, form prescribed in 50-16-512 - patients may examine and copy their health information.	**SAVA could:** 1. further examine whether Montana law should provide more transparency, notice, and access than HIPAA (be as specific as possible); 2. further examine Montana law to ensure match with HIPAA for the non-HIPAA entities; 3. take no further action with respect to this principle; or 4. take some other action regarding this principle

Table 3 - Health Information			
Principle	**Federal Law**	**Montana Law**	**Options**
3. Onward Transfer; Consistent Context (i.e, downstream use of information should be kept within purpose for which it was originally collected)	Health Insurance Portability and Accountability Act (HIPAA) - Pub. L. 104-191 Patients have the right to: - obtain a report on when and why their health information was shared for certain purposes; 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.	Uniform Health Care Information Act - Title 50, Ch. 16 Part 8 - Privacy Requirements - applies only to health care providers th t to HIPAA - more stringent than HIPAA in some cases, but less stringent than California - Erin MacLean stated that 50-16-812 - concerns when information is subject to compulsory disclosure process - violates HIPAA and needs to be fixed - 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	**SA** 1. further examine whether specific as possible); 2. further examine Montana law to ensure match with HIPAA for the non-HIPAA entities; 3. examine 50-16-812, MCA, and consider amendments so it does not violate HIPAA; 4. examine the business associates issue raised by Ms. MacLean; 5. take no further action with respect to this principle; or 6. take some other action regarding this principle

Table 3 - Health Information			
Principle	**Federal Law**	**Montana Law**	**Options**
4. Security	HITECH Act - 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.	Unfair Trade Practices Section 30-14-1704, MCA. Insurance Companies Section 33-19-321, MCA. - individuals must be notified of a security breach compromising their "medical record information" - consumer protection office under Dept. of Justice must also be notified	**SAVA could:** 1. further examine whether Montana law could better reflect the HITECH Act with respect to those entities not covered by HIPAA); 2. further examine Montana law to ensure match with HIPAA for the non-HIPAA entities; 3. take no further action with respect to this principle; or 4. take some other action regarding this principle
5. Data integrity; Verifiability; Right of consumer to correct or delete information	Health Insurance Portability and Accountability Act (HIPAA) - Pub. L. 104-191 - patients have the right to correct their health information.	Uniform Health Care Information Act - Title 50, Ch. 16 - patients may submit corrections to their health information.	**SAVA could:** 1. further examine whether Montana law should be stricter than HIPAA; 2. further examine Montana law to ensure match with HIPAA for the non-HIPAA entities; 3. take no further action with respect to this principle; or 4. take some other action regarding this principle

Table 3 - Health Information			
Principle	**Federal Law**	**Montana Law**	
6. Accountability; Enforcement	Health Insurance Portability and Accountability Act (HIPAA) - Pub. L. 104-191 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 HITECH Act - mandatory penalties for "willful neglect." - penalties were increased See Page 17 of Nov. 17 Staff Report	Uniform Health Care Information Act - Title 50, Ch. 16 Criminal and civil penalties are provided for in statute and the state attorney general or a county attorney is authorized to prosecute violations. Erin MacLean testified: - there isn't any policing and no state-level agency to field complaints - the penalties and fines in state statutes do not track with the federal penalties - CA could be a state to examine for stronger accountability and enforcement	**SAVA could:** 1. further examine whether Montana law should be stricter than HIPAA; 2. further examine Montana law to ensure match with HIPAA for the non-HIPAA entities; 3. consider state-level policing 4. consider state penalties matching the HIPAA and HITECH penalties 5. take no further action with respect to this principle; or 6. take some other action regarding this principle
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**
1. Control; Choice; Affirmative Consent (Opt-in); Right to Exit	Privacy Act of 1974 - 5 U.S.C. 552 et. seq. "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]. E-Government Act of 2002	State Agency Protection of Personal Information - Title 2, ch. 6, part 15, MCA See pages 23-24 in Nov. 17 staff report. Montana Information Technology Act - Title 2, ch. 17, part 5 - affirmative consent is required before a government website may collect personally identifiable information that will be passed on to a third party	**SAVA could:** 1. further examine federal law and compare it with Montana law 2. further examine Montana law 3. take no further action 4. take some other action
2. Transparency; Notice; Access		Montana Information Technology Act - Title 2, ch. 17, part 5 2-17-552 - government website - must generally describe information practices and operator's policies to protect privacy	**SAVA could:** 1. further examine federal law and compare it with Montana law 2. further examine Montana law 3. take no further action 4. take some other action

Table 4 - Government Information			
Principle	**Federal Law**	**Montana Law**	**Options**
3. Onward Transfer; Consistent Context (i.e, downstream use of information should be kept within purpose for which it was originally collected)		Montana Information Technology Act - Title 2, ch. 17, part 5 2-17-552 - 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	**SAVA could:** 1. further examine federal law and compare it with Montana law 2. further examine Montana law 3. take no further action 4. take some other action
4. Security		Montana Information Technology Act - Title 2, ch. 17, part 5 2-17-534 - Dept. of Administration (Chief Information Officer) - must develop guidelines and training for state agencies	**SAVA could:** 1. further examine federal law and compare it with Montana law 2. further examine Montana law 3. take no further action 4. take some other action

Table 4 - Government Information			
Principle	**Federal Law**	**Montana Law**	**Options**
5. Data integrity; Verifiability; Right of consumer to correct or delete information		Not addressed	**SAVA could:** 1. further examine federal law and compare it with Montana law 2. further examine Montana law 3. take no further action 4. take some other action
6. Accountability; Enforcement		2-17-514 - "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."	**SAVA could:** 1. further examine federal law and compare it with Montana law 2. further examine Montana law 3. take no further action 4. take some other action

Table 4 - Government Information			
Principle	**Federal Law**	**Montana Law**	**Options**

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

a. Uniform Health Care Information Act - Title 50, Ch. 16
Part 6 - Government Health Care Info.
- government entities with health care information must still comply with HIPAA
- Erin MacLean testified that the need to also comply with HIPAA should be clarified in the Part 6 statutes.

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.)?

c. Others?

ADMINISTRATION DISCUSSION DRAFT
CONSUMER PRIVACY BILL OF RIGHTS ACT

Bill

To establish baseline protections for individual privacy in the commercial arena and to foster timely, flexible implementations of these protections through enforceable codes of conduct developed by diverse stakeholders.

SEC. 1. Short Title. This Act may be cited as the Consumer Privacy Bill of Rights Act of 2015.

SEC. 2. Table of Contents.

SEC. 3. Findings. The Congress finds that:

(a) Americans cherish privacy as an element of their individual freedom.
(b) American laws, regulations, and enforcement entities provide robust privacy safeguards for consumers.
(c) There is rapid growth in the volume and variety of personal data being generated, collected, stored, and analyzed. This growth has the potential for great benefits to human knowledge, technological innovation, and economic growth, but also the potential to harm individual privacy and freedom.
(d) Laws must keep pace as technology and businesses practices evolve.
(e) Preserving individuals' trust and confidence that personal data will be protected appropriately, while supporting flexibility and the free flow of information, will promote continued innovation and economic growth in the networked economy.
(f) Enforcement of general principles in law will ensure that individuals continue to enjoy meaningful privacy protections while affording ample flexibility for technologies and business models to evolve.
(g) Enforceable codes of conduct developed through open, transparent processes will provide certainty for businesses and strong privacy protections for individuals.
(h) It is the sense of Congress that each covered entity should provide, when reasonable, a version of the notice required under this Act in a format that is computer-readable, to facilitate the development of information technology tools that will help individuals compare covered entities' personal data practices.

SEC. 4. Definitions.

(a) "Personal data"

(1) In General.—"Personal data" means any data that are under the control of a covered entity, not otherwise generally available to the public through lawful means, and are linked, or as a practical matter linkable by the covered entity, to a specific individual, or linked to a device that is associated with or routinely used by an individual, including but not limited to—
(A) the first name (or initial) and last name;

(B) a postal or email address;
(C) a telephone or fax number;
(D) a social security number, tax identification number, passport number, driver's license number, or any other unique government-issued identification number;
(E) any biometric identifier, such as a fingerprint or voice print;
(F) any unique persistent identifier, including a number or alphanumeric string that uniquely identifies a networked device; commercially issued identification numbers and service account numbers, such as a financial account number, credit card or debit card number, health care account number, retail account number; unique vehicle identifiers, including Vehicle Identification Numbers or license plate numbers; or any required security code, access code, or password that is necessary to access an individual's service account;
(G) unique identifiers or other uniquely assigned or descriptive information about personal computing or communication devices; or
(H) any data that are collected, created, processed, used, disclosed, stored, or otherwise maintained and linked, or as a practical matter linkable by the covered entity, to any of the foregoing.

(2) Exceptions.—
(A) De-identified data.—The term "personal data" shall not include data otherwise described by paragraph (1) that a covered entity (either directly or through an agent)—
(i) alters such that there is a reasonable basis for expecting that the data could not be linked as a practical matter to a specific individual or device;
(ii) publicly commits to refrain from attempting to identify with an individual or device and adopts relevant controls to prevent such identification;
(iii) causes to be covered by a contractual or other legally enforceable prohibition on each entity to which the covered entity discloses the data from attempting to link the data to a specific individual or device, and requires the same of all onward disclosures; and
(iv) requires each entity to which the covered entity discloses the data to publicly commit to refrain from attempting to link to a specific individual or device.
(B) Deleted data.—The term "personal data" shall not include data otherwise described by paragraph (1) that a covered entity deletes.
(C) Employee information.—The term "personal data" shall not include an employee's name, title, business address, business email address, business telephone number, business fax number, or any public licenses or records associated with the employment, when such information is collected or used by the employee's employer or another covered entity, in connection with such employment status.
(D) Cybersecurity data.—The term "personal data" shall not include cyber threat indicators collected, processed, created, used, retained, or disclosed in order to investigate, mitigate, or otherwise respond to a cybersecurity threat or incident, when processed for those purposes.

(i) The term "cyber threat indicator" means information—
(I) that is necessary to indicate, describe or identify—
(a) malicious reconnaissance, including communications that reasonably appear to be transmitted for the purpose of gathering technical information related to a cyber threat;
(b) a method of defeating a technical or operational control;
(c) a technical vulnerability;
(d) a method of causing a user with legitimate access to an information system or information that is stored on, processed by, or transiting an information system inadvertently to enable the defeat of a technical control or an operational control;
(e) malicious cyber command and control;
(f) any combination of (a)-(e).
(II) from which reasonable efforts have been made to remove information that can be used to identify specific persons reasonably believed to be unrelated to the cyber threat.

(b) "Covered entity"

(1) In General.—"Covered entity" means a person that collects, creates, processes, retains, uses, or discloses personal data in or affecting interstate commerce. Such term does not include—
(A) the Federal Government, the Government of any State, the Government of any Indian tribe, or any political subdivision, department, agency, component, entity, or instrumentality thereof;
(B) any employee, officer, agent, contractor, or organization working on behalf of an entity described in subparagraph (A), with regard to data processed on behalf of such entity;
(C) a natural person, unless acting in a non-de-minimis commercial capacity;
(D) any person that—
(i) collects, creates, processes, uses, retains, or discloses personal data of fewer than 10,000 individuals and devices during any 12-month period, or has 5 or fewer employees; and
(ii) does not knowingly collect, use, retain, or disclose any information that is linked with personal data and includes, or relates directly to, that individual's medical history; national origin; sexual orientation; gender identity; religious beliefs or affiliation; income, assets, or liabilities; precise geolocation information; unique biometric data; or Social Security number.
(iii) notwithstanding the foregoing, any person that is a covered entity solely because of clause (ii) shall be a covered entity only with regard to the data described in clause (ii).
(iv) notwithstanding the foregoing, any person described in clauses (i)-(ii) may elect to become a covered entity through public election;
(E) any person that has 25 or fewer employees, and would otherwise be a covered entity solely because of data that the person processes related to job applicants and employees in the ordinary course; or

(F) any other exceptions established pursuant to section 405 of this Act.

(2) Exception.—
(A) To the extent that a person collects, creates, processes, uses, retains, or discloses personal data needed to conduct research relating directly to security threats to or vulnerabilities in devices or networks, or to address threats or vulnerabilities identified by that research, such person shall not be deemed a covered entity for purposes of sections 101, 102, 103, 104, or 106 of Title I of this Act.
(B) This exception shall apply only so long as such person—
(i) uses such personal data exclusively for the activities described by subparagraph (A);
(ii) takes reasonable steps to mitigate privacy risks when conducting the activities permitted by subparagraph (A); and
(iii) destroys, deletes, or de-identifies such personal data within a reasonable time after such person has completed the activities permitted by subparagraph (A).

(c) "Collect" means acquire by any means, including but not limited to, direct or indirect interaction with an individual or purchase, lease, or rental.

(d) "Means to/of control" mean enabling individuals to make decisions about the processing of their personal data, including but not limited to, providing mechanisms to obtain consent, withdraw consent, correct inaccurate data, permit or restrict access to data, or otherwise identify and implement the privacy preferences of individuals.

(e) "Deletion" or "delete" means remove or destroy data (either directly or through an agent) such that there is a reasonable basis for expecting that the data could not be retrieved in the ordinary course. No requirement to delete, destroy, or de-identify data under this Act shall require a covered entity to delete, destroy, or de-identify data that are retained for backup or archival purposes to the extent that such systems are not accessed in the ordinary course. To the extent such backup or archival systems are accessed in the ordinary course, this Act's deletion requirements shall apply.

(f) "Minor" means an individual who is under 18 years of age.

(g) "Privacy risk" means the potential for personal data, on its own or when linked to other information about an individual, to cause emotional distress, or physical, financial, professional or other harm to an individual.

(h) "Commission" means the Federal Trade Commission.

(i) "State" includes the several States, the District of Columbia, Federally recognized Indian tribes, the Commonwealth of Puerto Rico, the Commonwealth of the

Northern Mariana Islands, American Samoa, Guam, the Virgin Islands, and any other territory or possession of the United States.

(j) "Customary business records" mean data, including personal data, typically collected in the ordinary course of conducting business and that is retained for generally accepted purposes for that business, including accounting, auditing, tax, fraud prevention, warranty fulfillment, billing, or other customary business purposes.

(k) "Context" means the circumstances surrounding a covered entity's processing of personal data, including but not limited to—

(1) the extent and frequency of direct interactions between individuals and the covered entity, if any;

(2) the nature and history of the interactions described in paragraph (1);

(3) the level of understanding that reasonable users of the covered entity's goods or services would have of how the covered entity processes the personal data that it collects, including through any notice provided by the covered entity;

(4) the range of goods or services that the covered entity offers, the use of such goods or services by individuals, the benefits of such goods or services to individuals, and the brand names that the covered entity uses to offer such goods or services;

(5) information known by the covered entity about the privacy preferences of individual users of its goods or services;

(6) the types of personal data foreseeably processed in order to provide a good or service that an individual requests from the covered entity;

(7) the types of personal data foreseeably processed in order to improve or market a good or service that an individual requests from the covered entity;

(8) the types of personal data foreseeably processed as customary business records;

(9) the age and sophistication of individuals who use the covered entity's goods or services, including whether the covered entity's goods or services are directed toward minors or the elderly;

(10) the extent to which personal data under the control of the covered entity are exposed to public view; and

(11) the extent to which personal data under the control of the covered entity are obscured.

(l) "Process personal data" or "personal data processing" means taking any action regarding data that is linked to an individual or a specific device, including but not limited to collecting, retaining, disclosing, using, merging, linking, and combining data.

(m) "Adverse action" has the same meaning as in section 701(d) of the Fair Credit Opportunity Act of 1974 (15 U.S.C. § 1691(d)(6)) and section 603(k)(1)(B)(i)-(iii) of the Fair Credit Reporting Act (15 U.S.C. § 1681a(k)(1)(B)(i)-(iii)).

(n) "Enumerated exceptions" means:

(1) Preventing or detecting fraud;

(2) Preventing or detecting child exploitation or serious violent crime;

(3) Protecting the security of devices, networks, or facilities;

(4) Protecting the rights or property of the covered entity or, upon consent of the customer, the covered entity's customer;

(5) Monitoring or enforcing agreements between the covered entity and an individual, including but not limited to, terms of service, terms of use, user agreements, or agreements concerning monitoring criminal activity;

(6) Processing customary business records (to the extent that such records are retained for reasonable periods of time or as legally required); or

(7) Complying with a legal requirement or responding to an authorized governmental request.

TITLE I—Privacy Bill of Rights

SEC. 101. Transparency.

(a) In General.—Each covered entity shall provide individuals in concise and easily understandable language, accurate, clear, timely, and conspicuous notice about the covered entity's privacy and security practices. Such notice shall be reasonable in light of context. Covered entities shall provide convenient and reasonable access to such notice, and any updates or modifications to such notice, to individuals about whom it processes personal data.

(b) Contents of Notice.—The notice required by subsection (a) shall include but is not limited to—

(1) The personal data the covered entity processes, including the sources of data collection if the collection is not directly from the individual;

(2) The purposes for which the covered entity collects, uses, and retains such personal data;

(3) The persons, or categories of persons, to which, and purposes for which, the covered entity discloses such personal data;

(4) When such personal data will be destroyed, deleted, or de-identified. If the covered entity will not destroy, delete, or de-identify personal data, it shall specify this in the notice;

(5) The mechanisms to grant individuals a meaningful opportunity to access their personal data and grant, refuse, or revoke consent for the processing of personal data;

(6) Whom individuals may contact with inquiries or complaints concerning the covered entity's personal data processing; and

(7) The measures taken to secure personal data.

(c) Trade Secrets.—Nothing in this section shall require a covered entity to reveal trade secret information. For the purposes of this subsection, "trade secret" is defined as stated in 18 U.S.C. § 1839. However, for the purposes of this subsection, the categories of personal data that a covered entity collects shall not be considered a trade secret.

SEC. 102. Individual Control.

(a) In General.—Each covered entity shall provide individuals with reasonable means to control the processing of personal data about them in proportion to the privacy risk to the individual and consistent with context.

(b) Manner of Providing Individual Control.—In providing the means of control pursuant to subsection (a), the covered entity shall offer mechanisms that are—

(1) reasonably accessible, understandable, and usable to individuals; and

(2) available at times and in manners that reasonably enable individuals to make decisions about the processing of their personal data.

(c) Withdrawal of Consent.—Each covered entity shall provide individuals a means to withdraw any consent granted under subsection (b) that is reasonably comparable to the means used to grant such consent.

(1) Deletion in response to withdrawal of consent.—Within a reasonable period of time that need not be less than 45 days after receiving an individual's withdrawal of consent for data retention, a covered entity shall delete the

personal data associated with the withdrawal of consent.

(2) Alternative means of compliance.—A covered entity may meet the requirement of this subsection by providing individuals with the means to request that the covered entity de-identify personal data pertaining to such individuals.

(3) Limitation on the obligation of covered entities.—The obligation of a covered entity under this subsection shall be limited to—

(A) Responding in a manner that is compatible with a legal obligation of the covered entity, or any applicable First Amendment interest of the covered entity in the personal data;

(B) Processing of personal data other than those specified in subsection (d); and

(C) Personal data under the control of the covered entity.

(d) Exceptions.—A covered entity shall not be subject to the requirements of subsection (a), subsection (c), or a requirement to provide heightened individual control under section 103(b)(1) of this Act, to the extent that the collection, creation, processing, retention, use, or disclosure of personal data is for purposes set forth in the enumerated exceptions.

(e) Material Changes.—Covered entities shall, upon any material changes to a practice or service that affect the prior or ongoing collection, use, dissemination, or maintenance of personal data—

(1) provide in advance clear and conspicuous descriptions of the changes; and

(2) with respect to previously collected personal data, provide individuals with compensating controls designed to mitigate privacy risks that may arise from the material changes, which may include seeking express affirmative consent from individuals.

SEC. 103. Respect for Context.

(a) In General.—If a covered entity processes personal data in a manner that is reasonable in light of context, this section does not apply. Personal data processing that fulfills an individual's request shall be presumed to be reasonable in light of context.

(b) Privacy Risk Management.—If a covered entity processes personal data in a manner that is not reasonable in light of context, the covered entity shall conduct a privacy risk analysis including, but not limited to, reviews of data sources, systems, information flows, partnering entities, and data and analysis uses to examine the potential for privacy risk. Covered entities shall take reasonable steps to mitigate

any identified privacy risks, which shall include, but are not limited to, providing heightened transparency and individual control.

(1) Heightened Transparency and Individual Control.—Covered entities shall provide individuals with notice regarding personal data practices that are not reasonable in light of context at times and in a manner reasonably designed to enable individuals to decide whether to reduce their exposure to the associated privacy risk, as well as a mechanism for control that is reasonably designed to permit individuals to exercise choice to reduce such privacy risk. The factors relevant to determining whether such notice and mechanism for control are reasonably designed shall include, but are not limited to—

(A) The placement and visibility of such notices, taking into account the size and capability of the device that will display the notice;

(B) The timing and frequency of such notices in relationship to when personal data is collected, used, and disclosed; and

(C) The relationship of the notice to the means that the covered entity provides to permit individuals to exercise control over personal data processing.

(c) Exception for certain personal data analysis.—Nothing in subsection (b) shall require a covered entity to provide heightened transparency and individual control when a covered entity analyzes personal data in a manner that is not reasonable in light of context if such analysis is supervised by a Privacy Review Board approved by the Federal Trade Commission and—

(1) The Privacy Review Board determines that it is impractical to provide heightened transparency and individual control;

(2) The Privacy Review Board determines that the goals of the covered entity's analysis are likely to provide substantial benefits that do not exclusively accrue to the covered entity;

(3) The Privacy Review Board determines that the covered entity has taken reasonable steps to mitigate privacy risks associated with the analysis, including risks associated with the absence of heightened transparency and individual control; and

(4) The Privacy Review Board determines that the likely benefits of the analysis outweigh the likely privacy risks.

(d) Disparate Impact.—When analyzing personal data in a manner that is not reasonable in light of context and results in adverse actions concerning multiple individuals, a covered entity shall—

(1) Conduct a disparate impact analysis to determine whether the analysis of personal data described in subsection (d) results in a disparate impact on individuals on the basis of age, race, color, religion, sex, sexual orientation, gender identity, disability, or national origin;

(2) Ensure that the scope, rigor, and sophistication of the disparate impact analysis are consistent with widely accepted analytic and technical practices; and

(3) Document the methodology and results of the disparate impact analysis and retain such documentation consistent with widely accepted analytic and technical practices.

(e) Rulemaking.—Within 180 days after enactment of this Act, the Commission shall promulgate regulations under 5 U.S.C. § 553 to establish the minimum requirements for Privacy Review Boards to qualify for Commission approval, forms and procedures for submission of applications for approval, and a process for review and revocation of such approval. When promulgating regulations under this subsection, the Commission shall consider, among other factors: the range of evaluation processes suitable for covered entities of various sizes, experiences, and resources; the range of evaluation processes suitable for the privacy risks posed by various types of personal data; the costs and benefits of levels of independence and expertise; the costs and benefits of levels of transparency and confidentiality; the importance of mitigating privacy risks; the importance of expedient determinations; and whether differing requirements are appropriate for Boards that are internal or external to covered entities. Within 90 days of receipt, following public comment, the Commission shall approve or deny an application for Privacy Review Board approval, and explain in writing the reasons for any denial.

(f) Appeals.—A person aggrieved may obtain review by a district court of the United States of appropriate jurisdiction, as provided for in 5 U.S.C. § 706 of—

(1) any Commission decision on an application submitted under subsection (c); or

(2) a failure by the Commission, within the period specified in subsection (e) to approve or deny an application for Privacy Review Board approval.

SEC. 104. Focused Collection and Responsible Use.

(a) In General.—Each covered entity may only collect, retain, and use personal data in a manner that is reasonable in light of context. A covered entity shall consider ways to minimize privacy risk when determining its personal data collection, retention, and use practices.

(b) A covered entity shall delete, destroy, or de-identify personal data within a reasonable time after it has fulfilled the purpose or purposes for which such personal data were first collected.

(c) Exceptions.—Nothing in this section shall be construed to prohibit a covered entity from collecting, creating, processing, retaining, using, or disclosing personal data for—

(1) Purposes set forth in the enumerated exceptions;

(2) Processing personal data if the covered entity provides heightened transparency and individual control in a manner that satisfies the requirements of section 103(b) of this Act; or

(3) Performing an analysis under the supervision of a Privacy Review Board pursuant to section 103(c) of this Act.

SEC. 105. Security.

(a) In General.—Each covered entity shall—

(1) identify reasonably foreseeable internal and external risks to the privacy and security of personal data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information;

(2) establish, implement, and maintain safeguards reasonably designed to ensure the security of such personal data, including but not limited to protecting against unauthorized loss, misuse, alteration, destruction, access to, or use of such information;

(3) regularly assess the sufficiency of any safeguards in place to control reasonably foreseeable internal and external risks; and

(4) evaluate and adjust such safeguards in light of the assessment in paragraph (3); any material changes in the operations or business arrangements of the covered entity; or any other circumstances that create a material impact on the privacy or security of personal data under control of the covered entity.

(b) Factors for safeguards.—The reasonableness of the safeguards that a covered entity adopts under subsection (a) shall be determined in light of—

(1) The degree of the privacy risk associated with the personal data under the covered entity's control;

(2) The foreseeability of threats to the security of such data;

(3) Widely accepted practices in administrative, technical, and physical safeguards for protecting personal data; and

(4) The cost of implementing and regularly reviewing such safeguards.

SEC. 106. Access and Accuracy.

(a) Access.—

(1) In General.—Each covered entity shall, upon the request of an individual, provide that individual with reasonable access to, or an accurate representation of, personal data that both pertains to such individual and is under the control of such covered entity. The degree and means of any access shall be reasonable and appropriate for the privacy risks associated with the personal data, the risk of adverse action against the individual if the data is inaccurate, and the cost to the covered entity of providing access to the individual.

(2) Limitations.—A covered entity shall not be required to provide such access if—
(A) the individual requesting access cannot reasonably verify his or her identity as the person to whom the personal data pertains;
(B) access by the individual to the personal data is limited by applicable law or legally recognized privilege, or any applicable First Amendment interest of the covered entity in that personal data;
(C) access by the individual would compromise a fraud investigation or a law enforcement, intelligence or national security purpose; or
(D) such request for access is frivolous or vexatious.

(b) Accuracy.—

(1) In General.—Each covered entity shall, in a manner that is reasonable and appropriate for the privacy risks associated with such personal data, establish, implement, and maintain procedures to ensure that the personal data under its control is accurate. In developing such procedures, the covered entity shall consider the costs and benefits of ensuring the accuracy of the personal data.

(2) Limitations.—The obligations in paragraph (1) do not apply to personal data that a covered entity obtains—
(A) From records made public by the Federal Government, the Government of any State, the Government of any Indian tribe, or any political subdivision of a State, provided that the covered entity at reasonable and regular intervals verifies that it is obtaining current versions of such sources; or
(B) Directly from the individual to whom the personal data pertains.

(c) Correction or Deletion.—

(1) In General.—Each covered entity shall, within a reasonable period of time after receiving a request from an individual, provide the individual with a means to dispute and resolve the accuracy or completeness of the personal data pertaining to that individual that is under the control of such entity. The means of resolving a dispute shall be reasonable and appropriate for the privacy risks and the risk of an adverse action against an individual that are associated with such personal data.

(2) Option to Decline Correction or Amendment.—When a covered entity uses or discloses personal data for purposes that could not reasonably result in an adverse action against an individual, the covered entity may decline to correct or amend the personal data. If the covered entity declines to correct or amend the personal data, the covered entity shall, upon request and authentication of the person making the request, destroy or delete the personal data that the covered entity maintains within a reasonable period of time that need not be less than 45 days, unless the data are exempt under subsection (b)(2)(A).

(3) Limitations.—A covered entity is not required under this subsection to—
(A) Fulfill a correction or deletion request when doing so would be incompatible with a legal obligation of the covered entity, or any applicable First Amendment interest of the covered entity in that personal data;
(B) Retain, maintain, reorganize, or restructure personal data;
(C) Correct personal data that it obtained under one or more of the conditions listed in subsection (b)(2)(A), except to the extent that an individual asserts that personal data derived from records made public by a governmental entity relate to a different individual; or
(D) Fulfill a deletion request if the data are processed or retained for purposes set forth in the enumerated exceptions.

(4) Additional Requirements Where Correction or Amendment Is Declined.—If the covered entity declines to correct or amend personal data at the request of an individual, and the covered entity obtained such personal data from another person or entity, the covered entity shall—
(A) correct any inaccuracy in the covered entity's records if the individual provides sufficient information to show that the personal data is incorrect; and
(B) inform the individual of the source of the data and, if reasonably available, where a request for correction may be directed.

(d) Activities Subject to the Fair Credit Reporting Act.—To the extent that the personal data pertaining to an individual is used for purposes covered by the Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*), covered entities subject to the Fair Credit Reporting Act shall be exempt from the requirements of section 106 of this Act.

SEC. 107. Accountability.

(a) In General.—Each covered entity shall take measures appropriate to the privacy risks associated with its personal data practices to ensure compliance with its obligations pursuant to this Act, including but not limited to—

(1) Providing training to employees who access, collect, create, use, process, maintain, or disclose personal data;

(2) Conducting internal or independent evaluation of its privacy and data protections;

(3) Building appropriate consideration for privacy and data protections into the design of its systems and practices; and

(4) Binding any person to whom the covered entity discloses personal data to use such data consistently with the covered entity's commitments with respect to the personal data and with the requirements set forth in Title I of this Act.

TITLE II.—Enforcement

SEC. 201. Enforcement by the Federal Trade Commission.

(a) Unfair or Deceptive Acts or Practices.—A violation of Title I of this Act shall be treated as an unfair or deceptive act or practice in violation of section 5 of the Federal Trade Commission Act (15 U.S.C. § 45).

(b) Powers of Commission—

(1) In General.—

(A) Any covered entity who violates this Act shall be subject to the penalties and entitled to the privileges and immunities provided in the Federal Trade Commission Act, except that liability for and the amount of civil penalties shall be governed by section 203 of this Act.

(B) Exception.—The Commission shall not bring an enforcement action for violations of Title I of this Act seeking civil penalties based on a covered entity's conduct undertaken within the first eighteen months after the date the covered entity first created or processed personal data.

(c) General Application.—The requirements of this Act apply to—

(1) those "persons, partnerships, or corporations" over which the Commission has authority pursuant to section 5(a)(2) of the Federal Trade Commission Act (15 U.S.C. § 45(a)(2)); and

(2) notwithstanding section 4 and section 5(a)(2) of that Act (15 U.S.C. §§ 44 and 45(a)(2)), any non-profit organization, including any organization described in section 501(c) of the Internal Revenue Code of 1986 that is exempt from taxation under section 501(a) of such Code.

(d) In enforcing this Act, the Commission shall not require the deployment or use of any specific products or technologies, including any specific device software or hardware.

SEC. 202. Enforcement by State Attorneys General.

(a) Civil Action.—If the attorney general of any State has reason to believe that the action of a covered entity in violation of Title I of this Act has caused or is causing harm to a substantial number of that State's residents, such attorney general may bring a civil action on behalf of those residents exclusively in an appropriate district court of the United States. Unless the Commission brings an action under section 201 of this Act or intervenes and prosecutes an action brought under this section, as described in subsections (b)(2)(A) and (b)(2)(B), the only remedy that may be sought or awarded in any action under this Act is injunctive relief, and nothing in this Act may be construed to provide for any other relief.

(b) Federal Trade Commission.—

(1) Notice to Federal Trade Commission.—At least 30 days prior to initiating any action under subsection (a), an attorney general shall provide the Commission with a copy of the entire court complaint and written disclosure of substantially all material evidence and information the attorney general possesses.

(2) Upon receiving notice from an attorney general of a proposed civil action, the Commission may—

(A) intervene as a matter of right as a party to that civil action;
(B) intervene as a matter of right as a party to that civil action and assume lead responsibility for the prosecution of the action; or
(C) permit the attorney general to proceed with the action without direct Commission participation.

(3) In the event that an attorney general believes that immediate action is necessary to protect the residents of the State from a substantial harm, the attorney general may request that the Commission expedite its review of the proposed action, and the Commission shall afford such request appropriate consideration as the circumstances may warrant.

(4) In any action brought under Title II of this Act, the district court, and any courts that review the district court's decision, shall accord substantial weight to the Commission's interpretations as to the legal requirements of this Act.

(c) Investigatory Powers.—Nothing in this section may be construed to prevent the attorney general of a State from exercising the powers conferred on such attorney general by the laws of such State to conduct investigations or to administer oaths or affirmations or to compel the attendance of witnesses or the production of documentary and other evidence.

SEC. 203. Civil Penalties.

(a) In General.—In an action brought by the Commission or prosecuted by the Commission pursuant to section 202(b)(2)(A) or section 202(b)(2)(B), in addition to any injunctive relief arising from a violation of Title I of this Act, the covered entity is liable for a civil penalty if the covered entity, with actual knowledge or knowledge fairly implied on the basis of objective circumstances, violates the Act. Both the amount of such civil penalty sought by the Commission and the amount of such civil penalty determined by the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require.

(1) The civil penalty shall be calculated by multiplying the number of days that the covered entity violates the Act by an amount not to exceed $35,000; or

(2) If the Commission provides notice to a covered entity, stated with particularity, that identifies a violation of this Act, the civil penalty shall be calculated by multiplying the number of directly affected consumers by an amount not to exceed $5,000, unless, within 45 days of receiving such a notice, the covered entity files with the Commission an objection that satisfies the requirements of subparagraph (A).

(A) An objection shall include an affidavit by the covered entity that to the best of the covered entity's knowledge, information, and belief, formed after an inquiry reasonable under the circumstances—

(i) it is not being filed for any improper purpose;
(ii) the defenses and other legal contentions are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law;
(iii) the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation; and
(iv) the denial of factual contentions are warranted on the evidence or, if specifically so identified, are reasonably based on belief or a lack of information.

(3) The total civil penalty determined by the court shall not exceed $25,000,000.

(b) Adjustment for Inflation.—Beginning on the date that the Consumer Price Index for All Urban Consumers is first published by the Bureau of Labor Statistics that is after 1 year after the date of the enactment of this Act, and each year thereafter, each of the amounts specified in subsection (a) shall be increased by the percentage increase in the Consumer Price Index published on that date from the Consumer Price Index published the previous year.

TITLE III.—Codes of Conduct to Implement the Consumer Privacy Bill of Rights

SEC. 301. Safe Harbor Through Enforceable Codes of Conduct.

(a) Commission Review of Codes of Conduct.—

(1) Beginning 1 day after the effective date of Commission regulations adopted under subsection (c), any person may apply to the Commission for approval of one or more codes of conduct governing the processing of personal data by a covered entity. Such application shall include—

(A) A description of how the proposed code provides equivalent or greater protections for personal data than are provided by the relevant section of Title I;

(B) A description of entities or activities the code is designed to cover;

(C) A description of the process by which the code was derived;

(D) A list of covered entities, if any are known at the time that the application under this subsection is made, that plan to adopt the code; and

(E) Such additional information as the Commission determines is appropriate.

(2) Timeline for Commission Review.—

(A) Department of Commerce Multistakeholder Processes.—The Secretary of Commerce may convene interested stakeholders, such as members of industry, civil society, the public safety community, and academia, to develop codes of conduct through an open, transparent process. The Commission shall approve or deny an application developed through a Department of Commerce multistakeholder process within 90 days after receipt.

(B) Within 120 days of receipt, and consistent with the other regulations adopted under subsection (c), the Commission shall approve or deny an application that concerns a code of conduct that was developed through a process that—

(i) Is open to all interested participants and allows them to participate on equal footing in the deliberations and discussions that lead to the code; and

(ii) Maintains transparency by, at minimum, making decisional documents readily available to the public at a time and in manner that permits meaningful review prior to any decision based upon such documents.

(C) Consistent with the other regulations adopted under subsection (c), the Commission shall approve or deny a code of conduct developed through any process not covered by subparagraph (A) or (B) within 180 days of receipt.

(3) Public Comment and Explanation of Decisions.—

(A) As soon as feasible after receipt of any proposed code of conduct, the Commission shall provide an opportunity for public comment on the code.

(B) The Commission shall publicly explain in writing the reasons for approving or denying each proposed code of conduct that it reviews pursuant to this section.

(4) Initial Approval.—The Commission shall approve an application only if the applicant demonstrates that the associated code of conduct—

(A) provides equivalent or greater protections for personal data pertaining to individuals than those provided by Title I of this Act; and

(B) contains provisions for periodic review of the code of conduct to ensure that it continues to provide sufficient protection over time for personal data pertaining to individuals.

(5) Presumption of Sufficiency.—Codes of conduct developed through a multistakeholder process pursuant to paragraph (2)(A) that meet the requirements established by the Commission shall be presumed to provide equivalent or greater protections for personal data as those provided by Title I of this Act. A Commission finding to the contrary shall be supported by a decision in writing.

(6) Duration.—

(A) No sooner than 3 years and no later than 5 years after approving a code of conduct, the Commission shall reassess such code. If the Commission determines that the code continues to provide equivalent or greater protections for personal data pertaining to individuals than those provided by Title I of this Act, in light of changes in consumer expectations, technology, and market conditions, the code shall continue to qualify as a safe harbor pursuant to subsection (d) for a period of no longer than 5 years following the determination.

(B) Notwithstanding subparagraph (A), the Commission, upon request or on its own motion, may reconsider an approval granted under paragraph (4). After receiving public comment, if the Commission determines, based on specific factors or evidence not available in the prior proceeding, that clearly demonstrate that a code of conduct does not or no longer provides equivalent or greater protections for personal data pertaining to individuals

than those provided by Title I of this Act, it shall withdraw its approval of such code of conduct.

(b) Non-Governmental Administration of Codes of Conduct.—

(1) Beginning 1 day after the effective date of Commission regulations adopted under subsection (c), any person may apply to the Commission for certification to administer and enforce one or more codes of conduct that have been approved by the Commission under subsection (a).

(2) The Commission shall approve an application only if an applicant demonstrates that it can effectively and expeditiously address and resolve alleged violations of each code of conduct administered by that applicant.

(3) Commission certification under this subsection shall be effective for no more than 5 years. The Commission, upon request or on its own motion, may review a person's administration of a code of conduct to determine whether, in light of changes in consumer expectations, technology, and market conditions, such person continues to provide adequate protection for individuals and their personal data. If the Commission determines, after receiving public comment, that a person's administration or enforcement of a code of conduct does not adequately protect individuals and their personal data, the Commission shall withdraw its certification under this subsection.

(4) Each year, each person certified by the Commission under this subsection shall submit to the Commission, in a form specified by the Commission, a report of its activities under this Title during the preceding year.

(c) Rulemaking.—Within 180 days after enactment of this Act, the Commission shall promulgate regulations under 5 U.S.C. § 553 to implement this Title, including regulations establishing—

(1) the minimum requirements for a process to qualify for the presumption in subsection (a)(5);

(2) procedural requirements for codes of conduct under subsection (a);

(3) procedural requirements for entities that wish to administer codes of conduct under subsection (b);

(4) forms and procedures for the submission of applications under subsections (a) and (b); and

(5) methods and procedures for receiving input from governmental agencies regarding the approval of codes of conduct, including procedures that govern submittal of classified or otherwise confidential information.

(d) Safe Harbor Protection.—In any suit or action brought under Title II of this Act for alleged violations of Title I of this Act, the defendant shall have a complete defense to each alleged violation of Title I of this Act if it demonstrates with respect to such an alleged violation that it has maintained a public commitment to adhere to a Commission-approved code of conduct that covers the practices that underlie the suit or action and is in compliance with such code of conduct.

(e) Appeals.—A person aggrieved may obtain review by a district court of the United States of appropriate jurisdiction, as provided for in 5 U.S.C. § 706 of—

(1) any Commission decision approving or denying an application submitted under subsections (a) or (b); or

(2) a failure by the Commission, within the periods specified in subsections (a)(2) and (c), to approve or deny a code of conduct.

TITLE IV.—Miscellaneous

SEC. 401. Preemption.

(a) In General.—This Act preempts any provision of a statute, regulation, or rule of a State or local government, with respect to those entities covered pursuant to this Act, to the extent that the provision imposes requirements on covered entities with respect to personal data processing.

(b) Safe Harbor Protection.—No State or local government may enforce any personal data processing law against a covered entity to the extent that that entity is entitled to safe harbor protection under section 301(d) of this Act.

(c) Protection of State Consumer Protection Laws.—This section shall not be construed to limit the enforcement by an attorney general or other official of a State of any State consumer protection law of general application and not specific to personal data processing.

(d) Protection of Certain State and Local Laws.—This Act shall not be construed to preempt the applicability of the following, to the extent that the claim in question is not based on a failure to comply with this Act—

(1) State or local laws that address the processing of health information or financial information;

(2) State or local laws that address notification requirements in the event of a data breach;

(3) State or local trespass, contract, or tort law;

(4) State or local laws that address the privacy of minors or K-12 students; or

(5) Other State or local laws to the extent that those laws relate to fraud or public safety.

SEC. 402. Preservation of Federal Trade Commission Authority.

(a) Deception.—Nothing in this Act shall be construed to limit the Commission's authority under section 5 of the FTC Act (15 U.S.C. § 41 *et seq.*) to prevent any deceptive act or practice relating to personal data processing.

(b) Unfairness.—Nothing in this Act shall be construed to limit the Commission's authority to prevent unfair acts or practices relating to personal data processing, except the conduct that underlies a claim by the Commission that a covered entity breached a commitment that it made as part of its adherence to a code of conduct approved under section 301 of this Act.

SEC. 403. Private Right of Action.

There shall be no private right of action under this Act, and nothing in this Act may be construed to provide a private right of action.

SEC. 404. Application with Other Laws.

(a) Rule of Construction.—Nothing in this Act shall be construed or applied so as to abridge the exercise of rights guaranteed under the First Amendment to the Constitution of the United States.

(b) Exemption for Certain Internet Intermediaries.—To the extent that a covered entity qualifies for protection under section 230(c) of the Communications Act of 1934 (47 U.S.C. § 230(c)), processing of personal data protected by section 230(c) is exempt from the requirements of this Act with regard to a request from a person other than the original "information content provider" as defined in 47 U.S.C. § 230(f)(3).

(c) Qualified Exemption for Persons Subject to Other Federal Privacy and Security Laws.—If a covered entity is subject to a provision of this Act and a comparable provision of a Federal privacy or security law described in subsection (d), such provision of this Act shall not apply to such person to the extent that such provision of Federal privacy or security law applies to such person.

(d) Effect on Other Federal Laws—

(1) Protection of Other Federal Privacy and Security Laws.—Nothing in this Act may be construed to modify, limit, or supersede the operation of privacy or security provisions in Federal laws, including those described in subsection (d), or the regulations established pursuant to such laws, or the provision of information

permitted or required, expressly or by implication, by such laws, with respect to Federal rights and practices.

(2) Effect on FTC Act.—Notwithstanding paragraph (1), the Federal Trade Commission Act shall be modified as described in Section 402 of this Act.

(e) The Federal privacy and security laws described in this subsection are as follows:

(1) Section 552a of title 5, United States Code (commonly known as the Privacy Act of 1974).

(2) The Right to Financial Privacy Act of 1978 (12 U.S.C. § 3401 *et seq.*).

(3) The Fair Credit Reporting Act (15 U.S.C. § 1681 *et seq.*).

(4) The Fair Debt Collection Practices Act (15 U.S.C. § 1692 *et seq.*).

(5) The Children's Online Privacy Protection Act of 1998 (15 U.S.C. § 6501 *et seq.*).

(6) Title V of the Gramm-Leach-Bliley Act (15 U.S.C. § 6801 *et seq.*).

(7) Chapters 119, 123, 206, and 121 of Title 18, United States Code.

(8) Section 2710 of Title 18, United States Code.

(9) Sections 444 and 445 of the General Education Provisions Act (20 U.S.C. §§ 1232g, 1232h), commonly known as the "Family Educational Rights and Privacy Act of 1974" and the "Protection of Pupil Rights Amendment," respectively.

(10) Sections 5701 and 7332 of Title 38, United States Code.

(11) The Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1320d-2 *et seq.*).

(12) The Privacy Protection Act of 1980 (42 U.S.C. § 2000aa *et seq.*).

(13) The provisions of part C of title XI of the Social Security Act, section 264 of the Health Insurance Portability and Accountability Act of 1996, and subtitle D of title IV of the Health Information Technology for Economic and Clinical Health Act, and regulations under such provisions.

(14) The E-Government Act of 2002 (44 U.S.C. § 101 *et seq.*).

(15) The Paperwork Reduction Act of 1995 (44 U.S.C. § 3501 *et seq.*).

(16) Federal Information Security Management Act of 2002 (44 U.S.C. § 3541 *et seq.*).

(17) The Communications Act of 1934, as amended (47 U.S.C. § 151 *et seq.*).

(18) The Communications Assistance for Law Enforcement Act (47 U.S.C. § 1001 *et seq.*).

(19) The Currency and Foreign Transactions Reporting Act of 1970, as amended (commonly known as the Bank Secrecy Act) (12 U.S.C. §§ 1829b and 1951-1959, 31 U.S.C. §§ 5311-5314 and 5316-5332), including the International Money Laundering Abatement and Financial Anti-Terrorism Act of 2001, Title III of P.L. 107-56, as amended.

(20) Executive Order 12333, as amended, "United States Intelligence Activities, July 30, 2008," and any successor orders.

(21) National Security Act of 1947.

(22) Foreign Intelligence Surveillance Act of 1978, as amended (50 U.S.C. § 1801 *et seq.*).

SEC. 405. Exceptions to the Definition of Covered Entity.

Rulemaking.—The Commission may promulgate regulations under 5 U.S.C. § 553 to establish additional exceptions from the definition of covered entity for categories of persons. When promulgating regulations under this section, the Commission shall consider, among other factors, the privacy risks posed by personal data processing by categories of persons of various sizes, experiences, resources, and types of commercial activity, including nonprofit activity; the importance of mitigating privacy risks; and the costs and benefits of including those categories of persons as covered entities. A person aggrieved by a regulation promulgated under this subsection may obtain review by a district court of the United States of appropriate jurisdiction, as provided for in 5 U.S.C. § 706. The Commission may modify or revoke such an exception in light of changes in consumer expectations, technology, and market conditions, but no sooner than 3 years after initial promulgation absent materially changed circumstances.

SEC. 406. Effective Date.

(a) The provisions of this Act will take effect as of the date of enactment.

(b) The obligations of covered entities under Title I of this Act shall not give rise to a cause of action based on this Act less than 2 years after the date of enactment of this Act.

SEC. 407. Severability.

If any provision of this Act, or the application thereof to any person or circumstance, is held unconstitutional or otherwise invalid, the validity of the remainder of the Act and the application of such provision to other persons and circumstances shall not be affected thereby.