Personal Information Ownership, Veteran Suicides, and Other Issues

A report to the 65th Legislature

December 2016

State Administration and Veterans' Affairs Interim Committee

2015-2016

This report summarizes the activities, research findings, and recommendations of the committee during the 2015-2016 interim.

Montana Legislative Services Division
PO Box 201706
Helena, MT 59620-1706
Phone: (406) 444-3064
FAX: 444-3036 http://leg.mt.gov

STATE ADMINISTRATION AND VETERANS' AFFAIRS INTERIM COMMITTEE 2015-2016

Before the close of each legislative session, the House and Senate leadership appoint lawmakers to interim committees. Under section 5-5-211, Montana Code Annotated, interim committees must be bipartisan and the appointing authority shall attempt to select not less than 50% of the members from the standing State Administration Committees and at least one member from the joint subcommittee that considers the related agency budgets.

MEMBERS

Senators	Representatives
Dee L. Brown (R) – Hungry Horse Presiding Officer	Bryce Bennett (D) – Missoula Vice Presiding Officer
Doug Kary (R) – Billings	Forrest Mandeville (R) – Columbus
Cliff Larsen (D) – Missoula	Wendy McKamey (R) – Great Falls
Jonathan Windy Boy (D) – Box Elder	Kathy Swanson (D) – Anaconda

STAFF
Sheri Scurr, Research Analyst
K. Virginia "Ginger" Aldrich, Staff Attorney
Katya Grover, Secretary

Legislative Services Division

PO Box 201706
Helena, MT 59620-1706
Phone: (406) 444-3064 FAX: 444-3036 Web: http://leg.mt.gov

TABLE OF CONTENTS

Statutory and Assigned Duties. . . . . Page 1

Executive Summary Of Recommendations. . . . . Page 2
House Joint Resolution 21 -
Study of Personal Information Ownership. . . . . Page 2
Veteran Suicide Prevention. . . . . Page 2
Elections. . . . . Page 3
Agency Oversight . . . . . Page 3

Chapter 1 - House Joint Resolution 21 Study
of Personal Information Ownership. . . . . Page 5
Purpose for Study. . . . . Page 5
Committee Activities. . . . . Page 6
The Big Data Ecosystem. . . . . Page 8
Current Law. . . . . Page 11
Information Ownership in Theory and Practice. . . . . Page 15
Policy Principles. . . . . Page 19
Consumer Information. . . . . Page 21
Financial Information . . . . . Page 28
Health Information. . . . . Page 31
Government Information. . . . . Page 35

Chapter 2 - Veteran Suicide Prevention. . . . . Page 39
Issue Background. . . . . Page 39
Committee Meetings. . . . . Page 40
Discussion and Action. . . . . Page 42

Appendix A - HJR 21. . . . . Page 45

Appendix B - Glossary of Internet Terms. . . . . Page 47

Appendix C - Glossary of Privacy Regulation Terms. . . . . Page 55

Statutory and Assigned Duties

Under sections 5-5-202, 5-5-211, 5-5-215, and 5-5-228 of the Montana Code Annotated, the State Administration and Veterans' Affairs Interim Committee conducts administrative rule review, program monitoring, and bill draft authorization for its assigned agencies.

The following agencies are assigned to the committee for oversight:

- Board of Veterans' Affairs (and the Montana Veterans' Affairs Division)
- Department of Administration (including the State Lottery Commission)
- Department of Military Affairs
- Office of the Commissioner of Political Practices
- Office of the Secretary of State
- Public Employees' Retirement Board
- Teachers' Retirement Board

The committee also conducts studies as assigned by the Legislative Council and examines any other emerging issues related to state administration, such as state contracting, state employee pay and classification, and state employee health benefits.

This interim, the committee's assigned study was the House Joint Resolution 21 (2015) study of personal information ownership. (See Appendix A)

The committee has special duties related to public employee retirement system oversight. As part of fulfilling these duties, the committee publishes the Legislator's Guide to Montana's Public Employee Retirement Systems, which is available on the committee's website.

Executive Summary Of Recommendations

House Joint Resolution 21 - Study of Personal Information Ownership

The committee reached general agreement that Montanans should have more ownership over their personal data and that they should be able to exercise their ownership rights as much as possible. However, the committee was unable to find a practical path forward at this time that would not have negative unintended consequences. The committee agreed this complicated issue deserves additional research. (See Chapter 1)

Veteran Suicide Prevention

LC 1031 — A bill revising the state suicide prevention program by further articulating that the program reach all ethnic groups and occupations, that the public awareness campaign be aimed at normalizing the need for all Montanans to address mental health problems, that media outreach include digital and social media, and specifying that veteran groups be solicited to provide input to the public awareness campaign. Providing $500,000 as a general fund appropriation to enhance the program. (See Chapter 2)

LC 1030 — A bill providing a general fund appropriation of $500,000 (as a starting point for further discussion during the session) for grants through the state suicide prevention office to local efforts targeted at veteran suicide prevention. (See Chapter 2)

LC 1029 — A bill requiring specified health and mental health care professions licensed in Montana to complete suicide assessment, treatment, and management training. (See Chapter 2)

Elections

LC0030 A bill to followup on HB 84 (2015), which generally revised election laws by standardizing administrative timelines and combining special purpose district elections with school district elections. This followup bill clarifies when an election requested by petition concerning a local government ordinance must be held, revises notice requirements related to resort tax elections, clarifies the deadline for write-in candidates in local government elections, revises the deadlines by which absentee and mail ballots must be available, clarifies the deadline for the cancellation of a conservation district election, clarifies that county election administrators rather than school district clerks perform voter registration duties for school elections, and clarifyies the transition of terms of office for special district officers. (More information is available on the committee's website accessible from www.leg.mt.gov.)

Agency Oversight

LC0086 This bill eliminates a statutory requirement for a state information technology report to the state administration and veterans' affairs interim committee. The report is still required to be made available to the Legislature under the provisions of section 2-17-522, MCA, and will continue to be provided to the Legislative Finance Committee under section 2-17-522, MCA. (More information is available on the committee's website accessible from www.leg.mt.gov.)

INTENTIONALLY BLANK

Chapter 1 -
House Joint Resolution 21
Study of Personal Information Ownership

Recommendation: The Committee reached general agreement that Montanans should have more ownership over their personal data and that they should be able to exercise their ownership rights as much as possible. However, the committee was unable to find a practical path forward at this time that would not have negative unintended consequences. The committee agreed this complicated issue deserves additional research.

Purpose for Study

HJR 21 was introduced in the 2015 session by Rep. Bryce Bennett (D - Missoula) representing House District 91. It was first heard in the House Judiciary Committee. In his opening statement, Rep. Bennett said the goal was to examine "ways in which we can conceptualize and legislate ownership over our personal information and data." [1] He noted that many organization gather information about us as we go about our day-to-day activities, for example doctors keep our sensitive information on file, grocery stores track what we buy with membership cards, and telecommunications companies track our locations through GPS applications on cell phones. The full text of the resolution is provided at Appendix A.

[1] Montana Legislature, House Committee on Judiciary, *Hearing on HJ 21*, 64th Regular Legislative Session, March 13, 2015. Audio file time 00:02:58.

Rep. Bennett boiled down the study tasks outlined in the resolution to two questions:

(1) To what extent do we own our personal data?
(2) If the information collected about us is our property, what rights come with that ownership?[2]

The study resolution's preamble notes that in this era of big data, personal information is being collected, used, and distributed to third parties in a manner not envisioned by individuals when they first shared their information. The preamble also states that there is confusion over who owns the information and to what extent an individual may control how the information is used and distributed.[3]

Committee Activities

Figure 1 outlines the committee's activities, staff reports, testimony received, and actions related to the HJR 21 study. Each meeting date is linked to the meeting materials web page from which the minutes log, staff reports, and other materials provided to the committee at that meeting may be accessed.

The audio and video files for each meeting are provided on the committee's home page, which is accessible by navigating from the Legislative Branch home page at www.leg.mt.gov to the 2015-16 interim committee web page and selecting the State Administration and Veterans' Affairs Interim Committee.

The committee requested one preliminary bill draft related to the study, LC 74, requiring commercial website to post privacy policies. However, the committee ultimately voted to not move forward with it as a committee bill.

[2] Ibid.

[3] The full text of the resolution is available at Appendix A. Online access to the resolution's history, including hearing dates, vote tallies, and available audio and video files of the hearings and floor debates on the bill is available by going to the Montana Legislative Branch home page at www.leg.mt.gov, navigating to the 2015 bills, and typing in "HJ 21".

Figure 1 - Committee HJR 21 Activities

** Note: The links in this table to the web page for each meeting date may not work during the time that the Legislative Branch website is being upgraded. If the links do not work, please visit www.leg.mt.gov to navigate to the actual web page to find the materials for each of the meetings listed.*

Meeting Date	Main Agenda Items/Reports	Committee Actions
Aug. 19, 2015	Organizational • Overview of HJR 21 • Review of committee's overall work plan	• Instructed staff to develop a study plan proposal giving equal weight to each study task and type of information, but that first clarified levels of ownership.
Nov. 17, 2015	Background Information • Staff Report: Big Picture Overview of Current Federal and State Law • Presentation: Role of Federal Trade Commission • Panel: Consumer Data • Presentation: Health Care Information • Panel: Financial Data • Presentation: State Government Data • Staff Report: HJR 21 Study Plan Proposal	• Adopted proposed study plan with change of moving examination of laws in other states to February meeting rather than April meeting.
Feb. 10, 2016	• Staff Report: Property Rights Theory, Policy Principles, and Options • Presentation: New Hampshire law on patient health information being "property"	The committee requested further research in the following areas: • Consumer data and online tracking • Financial information under Montana's current law • Health information and HIPAA compared to Montana law • State government information and agency compliance with online privacy policies.

Meeting Date	Main Agenda Items/Reports	Committee Actions
April 19, 2016	Consumer Information • Staff Reports: - Online Tracking: A Crash Course - Self-Regulation Framework - Requiring Notice - Requiring Opt-In • Stakeholder Roundtable Financial Information • Staff Report: Financial Service Providers - Current Law Exceptions Allowing for the Disclosure of Personal Information • Stakeholder Roundtable Health Information • Staff Report: HIPAA, Other States, and Certain Issues Regarding Montana's Laws • New Hampshire law follow-up • Stakeholder Roundtable Government Information • Staff Report: Exceptions to the Montana Information Technology Act • Stakeholder Roundtable	• Decided to send a letter to appropriate state and local entities requesting that state and local governmental entities be educated on the current state law requiring their web sites post online privacy policies. • Requested that the state Information Technology Services Division investigate state agency compliance with the online privacy policy requirement and report back to the committee. • Requested the drafting for further consideration a committee bill requiring commercial web sites that collect personal information to post privacy policies. The bill was to be based on certain provisions of the European Union and U.S. Privacy Shield framework, California online privacy laws, and a Utah act.
June 8, 2016	• Update on state agency compliance with current privacy policy law • Review of LC 74 - bill draft requiring commercial websites to post privacy policies • Stakeholder Roundtable on LC 74	• By majority vote (6-2), decided to not move forward with LC 74 as a committee bill.

The Big Data Ecosystem

In the background phase of its study, the committee examined the complex ecosystem that surrounds the collection, use, and distribution of personal data. This ecosystem penetrates all sectors of industry and both private and public entities. Data collectors include Internet browsers, social media networks, medical service providers, financial institutions, telecommunications companies, retail stores, online shopping networks, utility companies, and government agencies. In other words, certain data is being collected by nearly every Internet website or mobile device application. Data brokers buy and sell this data to analytics companies, online advertizing networks, credit bureaus, insurance companies, retail stores, medical research companies, and others. Government, law enforcement, and employment agencies are also part of this vast universe often called "big data". In sum, big data is big business.

According to analysts for CNN, in 2012, big data was a $300 billion-a-year industry and employed about 3 million people in the United States.[4]
E-commerce in the retail market alone is a significant part of the world economy. American consumers spent $186 billion through online transactions in 2010, and the number of online sales has been increasing dramatically since then. Worldwide, online retail spending was $1.6 trillion (USD) in 2015, and this spending is projected to keep growing by double digit rates each year for the foreseeable future.

[4] Jason Morris and Ed Vavandera, "Why big companies buy, sell your data," August 23, 2012, CNN.com.

A legislative staff report and a glossary of Internet terms presented to the committee on Feb. 10, 2016, provides additional information on this ecosystem.[5]

Source: LemonStand.com

[5] Sheri S. Scurr, "Online Tracking: A Crash Course", for the State Administration and Veterans' Affairs Interim Committee, Montana Legislative Services Division, Feb. 10, 2016. Includes a glossary of Internet terms. Also available online by navigating from www.leg.mt.gov.

Current Law

Overview

The committee examined current laws concerning the collection, use, and distribution of personal data and found the following:

- The current legal framework is a patchwork of federal and state laws and agencies.
- Most laws approach personal information in the context of privacy and security rather than ownership.
- Definitions of personal information vary depending on the industry or activity being regulated.
- Individual rights are often limited to the right to know about a company's information collection and management policies and practices rather than offering any real control or ownership of the information.
- States vary in how they approach personal information management issues, and approaches encompass a wide range of policy topics.
- California is a bellwether state for more restrictive laws that provided federally.

Federal Laws

Some of the main federal laws concerning the collection, use, and distribution of personal information are the following:

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

Montana Laws

In Montana, the following laws also apply and may be accessed online from www.leg.mt.gov:

- The Montana Unfair Trade Practices and Consumer Protection Act (Title 30, ch. 14, part 1, MCA).
- A prohibition against unfair or deceptive trade practices by insurers (section 33-180-102, MCA).
- The Insurance Information and Privacy Protection Act (Title 33, ch. 19, MCA).
- Impediment to identify theft (Title 30, ch. 14, part 1, MCA).
- State agency protection of personal information (Title 2, ch. 6, part 15, MCA).
- The Montana Information Technology Act (Title 2, ch. 17, part 5, MCA).

- Health care information (Title 50, ch. 16, MCA).
  - Uniform Health Care Information Act - Part 5.
  - Government Health Care Information Act - Part 6.
  - Health Care Information Privacy Requirements for Providers Subject to HIPAA - Part 8.

Other States

Several states are taking on the issue of personal data protection, ownership, and digital privacy. The following is a summary of information provided by the National Conference for State Legislatures (NCSL):

- In October 2015, California enacted the Electronic Communications Privacy Act (the California ECPA), which provides stricter protections that provided under federal law. The California ECPA requires, with some exceptions, that state governmental entities get a search warrant before obtaining or accessing electronic information stored on smart phones, tablets, laptops and other electronic devices. The electronic information includes e-mail, digital documents, photographs, passwords, geolocation data, and internet protocol (IP) addresses, which identify individual computers.[6]

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

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

[6] Link to California's website on privacy and online security laws https://oag.ca.gov/privacy/privacy-laws.

- In 2015, at least 32 state legislatures have considered or enacted legislation concerning notification about security breaches.

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

- The state of Delaware recently enacted four bills protecting the privacy of website and mobile application users, minors, students, and crime victims.[7]

The committee investigated whether other state laws have statutory language referring to personal information as property. New Hampshire was found to have a health information statute that uses the word "property" when referring to a patient's medical information:

> Section 332-I:1 Medical Records; Definitions. –
>
> I. All medical information contained in the medical records in the possession of any health care provider shall be deemed to be the *property* of the patient. The patient shall be entitled to a copy of such records upon request. The charge for the copying of a patient's medical records shall not exceed $15 for the first 30 pages or $.50 per page, whichever is greater; provided, that copies of filmed records such as radiograms, x-rays, and sonograms shall be copied at a reasonable cost. [emphasis added]

[7] Link to NCSL website about online privacy and security: http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-and-security.aspx.

The law was enacted in 1989. However, further inquiry into the history and application of this statute did not determine whether this language provided individuals more control over their personal information than if the word "property" were not used. Also, an effort to examine the legislative history of this statute did not reveal why the word "property" was used.

More Information

A legislative staff report presented to the committee on Nov. 17, 2015, provides an in-depth review of some of the key federal laws, Montana's laws, and the laws in some other states.[8]

Information Ownership in Theory and Practice

Ownership Issue or Privacy Right?

Many legal scholars contrast ownership rights with privacy rights and argue that laws approaching personal information from an ownership perspective would give individuals more control than privacy and security laws. However, they acknowledge that ownership theories also fall short in some respects.[9]

There is wide agreement, however, that the current patchwork of sector-specific privacy and security laws offers insufficient protections for individual rights and that improvements need to be made in how these rights are articulated and honored.[10]

---

[8] Sheri S. Scurr, "Overview of Federal and State Laws", for the State Administration and Veterans' Affairs Interim Committee, Montana Legislative Services Division, Nov. 17, 2015. Also available online by navigating from www.leg.mt.gov.

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

[10] 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.

Ownership Concepts

The committee reviewed research showing that the concept of ownership of personal information is itself multi-faceted and can be discussed in different ways, such as:

- a bundle of rights, with some rights "running with" the information even after it is transferred, similar to covenants that remain on a parcel of land even after the land is sold;[11]
- similar to ownership of intellectual property;[12]
- a commodity that is bought and sold in a market place;[13]
- an inalienable human right to define one's own identity;[14] and
- a right that confers power to control how the property is used.[15]

Information As Property: Simple Premise, Complex Application

Approaching one of the various concepts of ownership, the concept of personal information being property upon which certain covenants or restrictions are placed, seems simple enough. However, a legislative staff review of literature concerning this approach revealed that the issue becomes complex when the information is aggregated with other information collected differently and when proprietary technology is applied.[16]

---

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

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

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

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

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

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

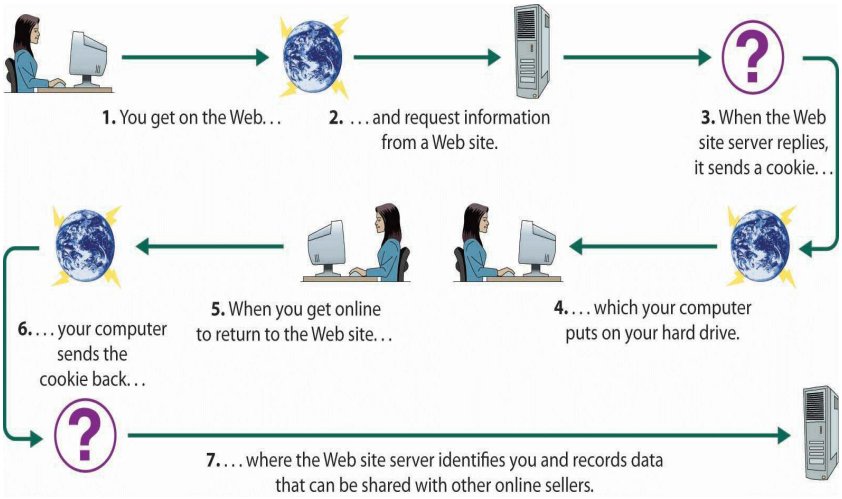
For example, a person browses the Internet for cowboy boots. The person's computer identification number, known as an Internet Protocol (IP) address, and the person's interest in cowboy boots is collected by the web browser. The browser is the property of the company that owns the technology, such as Google. If Google owns the search results, does it own the personal information collected from the search?

The data collected is transferred a data broker where other browsing history from the same IP address is added (via a proprietary database technology) to a database where it is aggregated with other information collected related to the same IP address. How is a property right that "runs with the IP address" to be differentiated when the IP address itself is gained at various times through various methods? And, how is an individual right to the IP address to be balanced with the rights of the company that owns the proprietary technology that allows for the information to be aggregated and sorted?

The data broker then sells the aggregated data to an analytics company. The analytics company applies its patented algorithms to develop a profile of the consumer as a middle-aged female home owner in Billings, Montana, who belongs to a fitness center, likely has a $60,000-a-year household income, and lives in a household with two teenage daughters. If the data collector offered the consumer the right to "opt-out" of certain types of uses for the data, does this caveat also get transferred to the analytics company? If so, then how does the company segregate the consumer's choice from other choices the consumer may have made when browsing a different website?

The analytics company then sells the consumer profile to an Internet marketing company. The marketing company has various clients, including Western wear companies, health products retailers, horse trailer manufacturers, and auto dealers. The marketing company has an Internet ad affiliate that specializes in serving Internet ads to consumers when they browse the Internet. So, this profile is again shared.

The net result of all of these transactions is that while the consumer is browsing the Internet or posting on social media, the consumer sees ads not only for cowboy boots, but also for horse trailers, teen clothing, fitness products, refinancing home loans, and pick-up trucks.



Source: www.flatworldknowledge.com

When data was initially collected, did the individual have a right to know that the data would eventually be sold and shared with the Internet ad company and other retailers? And, does the consumer have the right to choose whether or that information (collected by proprietary technology) is sold to an ad company? If so, how is the consumer's choice to be exercised in practical terms before the transactions have ever taken place? And, in all of these transactions, what actually remains the property of the consumer after the information was aggregated, analyzed, and redistributed by technology owned by the data broker, analytics, and marketing companies?

International Complexities

The scenario described above gets even more complex when you consider that the laws of other nations may also come into play. The laws applicable to

information collected on a European citizen, for example, are different than the laws applicable to a U.S. citizen. Under laws applicable to members of the European Union, companies must post online privacy policies, allow consumers to opt-out of data collection, and ensure that any companies that buy the consumer's personal data comply with the same policies. However, these requirements are not law in the United States. Therefore, there is an international framework called the EU-U.S. Privacy Shield whereby a U.S. company collecting data on a European consumer may certify to the Federal Trade Commission and U.S. Department of Commerce compliance with these provisions.

Policy Principles

Laws for Some, Guidelines for Others

To help companies navigate the complexities of how personal data must be managed in the context of various inconsistent state, federal, and international laws, government agencies and private organizations have developed some basic policy principles.[17]

These basic principles, which are law in the European Union[18], voluntary guidelines in the United States[19], and best practice standards for member companies of various U.S. business associations[20], are as follows:

---

[17] Sheri S. Scurr, "HJR 21 Study of Personal Information Ownership: Property Rights Theory, Policy Principles, and Options for Further Research," for the State Administration and Veterans' Affairs Interim Committee, Montana Legislative Services Division, Feb. 10, 2016. Also available online by navigating to the committee's website from www.leg.mt.gov.

[18] Information about the EU-U.S. Privacy Shield is available from the U.S. Department of Commerce at https://www.privacyshield.gov/welcome.

[19] For more information on Fair Information Practice Principles used by many U.S. government agencies that offer best practice guidelines to business for a voluntary compliance program, see https://en.wikipedia.org/wiki/FTC_Fair_Information_Practice.

[20] Examples of business associations that offer standards of practice and a self-regulatory framework are the Digital Advertising Alliance, the Network Advertising Initiative, and the Interactive Advertizing Bureau.

- Notice - Individuals should be informed that their data is being collected and about how it will be used.

- Choice - Individuals should at least have the option to opt out of (if not be required to opt in to) the collection and the forward transfer of the data to third parties.
- Onward Transfer - Transfers of data to third parties should only occur to other organizations that follow adequate data protection principles.

- Security - Reasonable efforts should be made to prevent loss of collected information.

- Data Integrity - Data collected and transferred should be relevant and reliable and used only for the purpose for which it was collected, even when transferred to third parties.

- Access - Individuals should be able to access information held about them and correct or delete inaccurate information.

- Enforcement - There should be an effective means of enforcing these rules.

More Information

A legislative staff report presented to the committee on April 19, 2016, provides additional information on the self-regulatory framework in the United States and the various federal and international organizations involved in establishing policy principles for member nations and companies.[21]

[21] Sheri S. Scurr, "Self Regulation and the Online Collection of Personal Information for Behavioral Advertizing" and for the State Administration and Veterans' Affairs Interim Committee, Montana Legislative Services Division, April 19, 2016. Also available online by navigating to the committee's website from www.leg.mt.gov.

Consumer Information

Research

At it's Feb. 10, 2016, meeting, the committee requested further research as follows:

- Requiring web sites to inform users of information practices.
- Requiring that a consumer must "opt-in" before a business may collect, use, or share the consumer's information.
- Requiring that individuals be allowed to access and correct or delete their personal information.
- Tightening Montana's security breach notification laws.
- Enforcement options.

At its April 19, 2016, meeting, the committee received staff research papers[22] detailing the notice and opt-in laws or voluntary best practices adopted by the following entities:

- EU-U.S. Privacy Shield.
- Asia-Pacific Economic Cooperation.
- Organization for Economic Cooperation and Development.
- Federal Trade Commission (FTC).
- Internet Policy Task Force, U.S. Department of Commerce.
- Digital Advertising Alliance.
- Network Advertising Initiative.
- Interactive Advertising Bureau.
- California.
- Connecticut
- Delaware
- Utah.

[22] See Sheri S. Scurr, "Issue Brief #1 - Requiring Notice of Online Information Collection Practices" and "Issue Brief #2 - Requiring Opt-In For Online Data Collection For Marketing", for the State Administration and Veterans' Affairs Interim Committee, Montana Legislative Services Division, April 19, 2016. Also available by navigating to the committee's website from www.leg.mt.gov.

The reports note that Montana does not currently require online commercial entities to post a privacy policy or require online companies to offer an opt-in choice to clients. Rather, Montana mirrors the FTC approach by prohibiting unfair and deceptive trade practices. Montana's Consumer Protection Act is Part 1 , of Chapter 14, in Title 30 (Trade and Commerce). The key statute, section 30-14-103, MCA. Unlawful practices, states: "Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful."

Due to time constraints, staff research reports were not completed on requiring that individuals be allowed to access and correct or delete their personal information, tightening Montana's security breach notification laws, or enforcement options.

Discussion and Preliminary Action

After the research and testimony presented at the April 19, 2016, committee meeting, Rep. Bryce Bennett offered an outline of what could be included in a committee bill to require commercial web sites that collect personal information on Montana consumers to conspicuously post privacy policies. He proposed that these privacy policies inform users of what information would be collected, how it would be used, whether it would be disclosed to third parties, how to contact the organization with inquiries or complaints, what rights an individual had, and the choices and means available to the individual for limiting the use and disclosure of the information. His proposal also included instructions about how the notice was to be provided and empowered the Office of Attorney General to enforce the provisions. The enforcement provision included language stating that an enforcement action could commence if the web site failed to come into compliance within 30 days of notification about noncompliance. The language of Rep. Bennett's proposal was based on California privacy laws and the EU-U.S. Privacy Shield .[23]

[23] Ibid., 08:21:00 and Exhibit 27.

Rep. Forrest Mandeville handed out copies of the Utah "Notice of Intent to Sell Nonpublic Personal Information Act", and suggested that the committee bill could incorporate the best parts of the act. He noted that the Utah law was not limited to online transactions. Rep. Mandeville also said he liked the civil liability section of the act that included a fine for each violation with enforcement by a private civil action rather than a government agency.[24]

Committee members discussed various enforcement options and ways to provide penalties, especially with respect to international corporations. Legal staff clarified that a website would have to be directed toward Montana consumers before a state court would determine it had jurisdiction.

Rep. Bennett offered comments on some of the provisions of the Utah law he said were unclear to him or that he thought should be further fleshed out or not included.

Rep. Bennett moved for staff to draft a bill compiling the provisions included in his outline and the provisions of the Utah law, except for the Utah provision related to oral contracts. Discussion on the motion clarified that there would be both a provision for enforcement by the Office of Attorney General and a provision for a private right of action. The motion passed unanimously, with Rep. Windy Boy excused.

Based on the motion, staff drafted LC 74 for the committee's further consideration at the April 19, 2016, meeting. The text of LC 74 along with staff notes on the drafting of LC 74 is available on the June 8, 2016, committee meeting webpage.

[24] Ibid., 08:27:00 and Exhibit 28.

Testimony

April 19, 2016

Charles Denowh presented testimony on behalf of the Internet Coalition[25], a national trade association that provides information on state government affairs to member companies, and NetChoice[26], an association of e-commerce businesses and online consumers. The highlights of his testimony were as follows:

- He pointed to existing federal laws and enforcement actions as well as the commitment that he said online businesses already have to enhancing privacy and security protections for their clients. The testimony opposed requiring an opt-in regime and suggested that Internet advertising companies could see a $33 billion decline in the first 5 years if such a requirement were enacted.

- He warned against Montana creating "devastating new regulations" for online service providers.

- Mr. Denowh concluded with a statement that Montana should not emulate the "mistakes made by the European Union".[27]

Marcus Meyer of the Office of Consumer Protection, Department of Justice, offered informational testimony about how his office provided information to help consumers prevent identity theft and how his office provides an identity theft "passport" to help victims of identity theft recover after an identity theft.[28]

---

[25] For more information about the Internet Coalition, see http://www.theinternetcoalition.com/.

[26] For more information about NetChoice, see https://netchoice.org/.

[27] State Administration and Veterans' Affairs Interim Committee, Minutes, Montana Legislative Services Division, April 19, 2016, Exhibit 6, audio/video time 01:50:49.

[28] Ibid., audio/video time 01:55:00.

Brad Griffin, president of the Montana Retail Association, a statewide trade association representing about 800 companies including retailer, restaurants, and tire and equipment dealers, provided testimony that may be summarized as follows:

- Each of us is responsible for our own online privacy.
- Many national and international organizations already adhere to best practices guidelines, but the technological landscape is ever-changing, so a law providing specific requirements would be unwise.
- He does not think that California is actively enforcing its privacy laws nor is active enforcement occurring in New York.
- A Montana notice or opt-in requirement would have international implications and be difficult on businesses.[29]

June 8, 2016 - Testimony on LC 74

Proponents:

Proponents of privacy policies say that privacy policies simply require that organizations disclose how they handle personal information and are essential to protecting consumer rights. Privacy policy advocates state that privacy policies are required under the EU-U.S. Privacy Shield, are commonly accepted by most industry leaders as a best practice, do not have to be complicated or expensive to produce, that numerous resources are available to help organizations develop these policies, and that any organization that collects personal information should already have a policy about how the information is to be handled so ensuring that consumers are informed is just common sense.

[29] Ibid., audio/video time 01:56:00.

Some of the organizations that advocate for online privacy policies include the following:

- Electronic Privacy Information Center, https://epic.org/
- Electronic Frontier Foundation, https://www.eff.org/
- Consumers Union, http://consumersunion.org/

Opponents:
Steve Turkiewicz of the Montana Bankers' Association testified that federal law and regulations under the federal Gramm-Leach-Bliley Act are very explicit and extensive about what information must be provided by financial institutions to clients. He asked that the bill draft not encompass financial institutions.

Brad Griffin of the Montana Retail Association expressed concern about language in the bill draft about individuals notifying the appropriate party of a complaint and about the fine structure.

Carl Szabo, a privacy law specialist representing NetChoice.org, said he understood the concerns giving rise to the bill draft, but the industry is moving away from privacy policies because they are lengthy and difficult to understand and that consumers usually do not read them. He said there are better ways to inform consumers. Mr. Szabo also stated that to comply with the bill, businesses would have to hire expensive attorneys to draft the policies and that by drafting the policies, businesses are exposing themselves to liabilities. He also said that the definition of what is personally identifiable information is constantly changing. He said that the California law requiring privacy policies has never been enforced in its 12-year history. In answering questions from committee members, Mr. Szabo talked about the "just-in-time" approach where applications have pop-up notifications alerting consumers that the application will be collecting information and asking for permissions.

Matt Dale of the Office of Consumer Protection, Montana Department of Justice, provided informational testimony that the office has not received any complaints related to privacy policies.

Shelby DeMars of the Internet Coalition testified that the committee's preliminary bill as drafted unfairly targets commercial websites. She said the bill would have significant financial implications for businesses, especially smaller businesses. Ms. DeMars also said technology is advancing rapidly and that better ways are being developed to inform consumers about their rights concerning personal information.

Kelly O'Sullivan, legal counsel for the Montana Division for Banking and Financial Institutions said that the division regulates financial institutions in Montana and that the enforcement provisions in the bill draft that give the Office of Attorney General enforcement authority would be redundant.

Discussion and Action on LC 74

Some committee members expressed concern about government regulation, how the bill would be enforced, the financial burden on the businesses, and the fast-pace of technological advances, and said that the bill may have unintended consequences. Other committee members said pop-up notifications cannot provide all of the information consumers should be able to access, that the bill would not be too much of a burden on businesses, that it is also important to protect the rights of consumers, and that technology is not going to change so much that the bill would be outdated.

There seemed to be general agreement that online privacy was an important issue and likely to continue to be a key policy concern for legislators.

Sen. Dee Brown moved that the committee not forward LC 74 as a committee bill. The motion passed 6-2 with Rep. Bryce Bennett and Sen. Jonathan Windy Boy voting "no".[30]

[30] State Administration and Veterans' Affairs Interim Committee, Minutes, Montana Legislative Services Division, June 8, 2016, audio/video time 05:09:16 for the start of the discussion.

Financial Information

Research

With respect to financial information, at its Feb. 10, 2016, meeting, the committee chose to further examine:

- The Montana's current law allowing for the sharing of certain information to be shared without the client's affirmative consent.
- Tightening Montana's security breach notification laws.
- Enforcement options.

At its April 19, 2016, meeting, the committee received a staff research paper responding to the committee's information request. The paper covered Montana's current law, federal law, and laws in other states.[31]

The following are some of the highlights of the paper:

- Montana Insurance Information and Privacy Protection Act was enacted in 1981 and is administered by the State Auditor's Office. Under the act, certain insurance businesses are prohibited from sharing a customer's personal information, except as specified in the act. In other words, personal information may be disclosed only for specified purposes and only under specified circumstances. In all cases, a customer's personal information may be shared only with the written authorization of the customer (i.e., by an "opt-in" affirmative consent).

[31] Sheri S. Scurr, "Financial Services Providers: Current Law Exceptions Allowing for the Disclosure of Personal Information" for the State Administration and Veterans' Affairs Interim Committee, Montana Legislative Services Division, April 19, 2016. Also available online by navigating to the committee's website from www.leg.mt.gov.

- The Financial Services Modernization Act (Gramm-Leach-Baily Act (GLBA)) (15 U.S.C. 6801 through 6827) is the primary privacy law governing the financial industry. The law was originally enacted in 1999, more than 17 years after Montana's Insurance Information and Privacy Protection Act, but a few years before Montana's code section authorizing disclosure of personal information for marketing purposes. The FTC's regulation implementing the act is called the Financial Privacy Rule.

- California's Financial Information Privacy Act:
  - Prohibits financial institutions from sharing or selling personally identifiable nonpublic information without obtaining a consumer's consent, as provided.
  - Requires a plain-language notice of the privacy rights it confers.
  - Requires that a consumer must "opt in" before a financial institution may share personal information with an unaffiliated third party.
  - Requires that consumers be given an opportunity to "opt out" of sharing with a financial institution's financial marketing partners.
  - Requires that consumers be given the opportunity to "opt out" of sharing with a financial institution's affiliates, with some exceptions.
  - When an affiliate is wholly owned, in the same line of business, subject to the same functional regulator and operates under the same brand name, an institution may share its customers' personal information with the affiliate without providing an opt-out right.

Testimony

Nick Mazanec, staff attorney for the State Auditor's Office, provided a copy of and briefly discussed a draft of a model law from the National Association of Insurance Commissioners entitled "Insurance Data Security Model Law". He said the State Auditor's Office would be supporting this act as a good attempt to address data security, breach notification, and identity theft protection issues. With respect to current Montana law, he stated that the State Auditor's Office had great confidence in the soundness of current law and that even though it was originally enacted in 1981, the act has been regularly updated. He said Montana's law is stronger than the federal law because it requires an "opt-in" process rather than the opt-out framework under federal law. Mr. Mazanec said the office has identified some concerns regarding data breach notification laws and would be supporting state legislation to require that data breaches be reported sooner.

Mr. Mazanec also said the State Auditor's Office is concerned about federal legislation currently being considered by Congress (the Data Security Act of 2015) that would preempt state regulation concerning data breaches.[32]

Jacqueline Lenmark, representing the American Insurance Association, the American Council of Life Insurers, and Aflac, testified that Montana law was crafted deliberately and takes a very thorough and careful approach to consumer protection in the financial and insurance industry. She said Montana's current law is also closely coordinated with current federal law. Ms. Lenmark said that the crafting of Montana's law was a consensus effort and that any amendment to it would have to be looked at very carefully.[33]

Kelly O'Sullivan, legal counsel, Division on Banking and Financial Institutions, Department of Administration, stated that banking is a heavily regulated act and

[32] State Administration and Veterans' Affairs Interim Committee, Minutes, Montana Legislative Services Division, April 19, 2016, audio/video time 02:26:33.

[33] Ibid., audio/video time 02:36.14.

that the state operates with the federal GLBA and the Fair Credit Reporting Act, which preempt state law. She said any work the committee would do in this area would need to be done with a great deal of precision.[34]

Steve Turkiewicz, president/CEO, Montana Bankers Association, also testified about how the financial industry is heavily regulated. He also commented on how the financial industry must cooperate with law enforcement agencies and on the host of federal agencies that have complex regulations that govern financial institutions in the state.[35]

Discussion and Action

Committee discussion noted the amount of scrutiny the financial industry already gets, that most regulation is federal and that some federal laws preempt state laws, and that the committee needed to narrow its focus. Sen. Dee Brown moved that financial information not be further considered by the committee. The motion passed unanimously by voice vote with Sen. Windy Boy excused.[36]

Health Information

Research

With respect to health information, the committee chose to further examine:

- Whether Montana health information law should be more stringent than the federal HIPAA (Health Insurance Portability and Accountability Act).
- Whether and how to make the law consistent with respect to health care entities that are not covered by HIPAA.

[34] Ibid., audio/video time 02:40.43.

[35] Ibid., audio/video time 02:42.20.

[36] Ibid., audio/video time 02:48.50.

- Section 50-16-812, MCA, and consider amendments that would ensure the statute does not violate HIPAA.

- How to address and define business associates with respect to the sharing of protected health information.

- How best to provide for state-level policing and enforcement and consider amendments that would make state penalties at least match the federal penalties for violations.

At its April 19, 2016, meeting, the committee received a staff research paper responding to the committee's information request. The paper covered HIPAA, other states, and certain portions of Montana's current law.[37]

The following are some of the highlights of the paper:

- HIPAA is the Health Insurance Portability and Accountability Act of 1996. The U.S. Department of Health and Human Services was required to implement the act. To cover the privacy provisions of the act, HHS adopted what is referred to as the Privacy Rule. The HHS website summarizes the Privacy Rule as follows: The HIPAA Privacy Rule establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients rights over their health information, including rights to examine and obtain a copy of their

[37] Sheri S. Scurr, "Health Information: HIPAA, Other States, and Certain Issues Regarding Montana's Laws" for the State Administration and Veterans' Affairs Interim Committee, Montana Legislative Services Division, April 19, 2016. Also available online by navigating to the committee's website from www.leg.mt.gov.

health records, and to request corrections. A summary of the key provisions of HIPAA and the Privacy Rule is available online.

- Many states have health information laws applicable to pharmacies that are, in certain cases, stricter than HIPAA. Walmart maintains a web page that provides state-by-state information about the privacy practices applicable in each of these states.[38]

States with Pharmacy Information Laws Stricter than HIPAA		
Alabama	Massachusetts	Puerto Rico
Arizona	Michigan	Rhode Island
California	Missouri	South Carolina
Connecticut	Montana	South Dakota
Florida	New Hampshire	Tennessee
Georgia	New Jersey	Texas
Hawaii	New Mexico	Utah
Idaho	New York	Vermont
Indiana	North Carolina	Washington
Iowa	North Dakota	West Virginia
Kentucky	Ohio	Wisconsin
Maine	Oklahoma	Wyoming
	Pennsylvania	

- Areas of Montana law identified as appropriate for additional examination if the committee wished to focus on health information ownership rights included:
  - Title 50, chapter 16, part 5 - Uniform Health Care Information
  - Title 50, chapter 16, part 6 - Government Health Care Information
  - Title 50, chapter 16, part 8 - Health Care Information Privacy Requirements for Providers Subject to HIPAA.

[38] Walmart pharmacy web page with by-state HIPAA information: http://corporate.walmart.com/privacy-security/notices/pharmacy-privacy-practices-state-law-supplement

Testimony

Dick Brown, president/CEO, Montana Hospital Association, explained oversight provided through federal agencies. He stated that the health information is more heavily regulated than the financial industry. Mr. Brown also discussed security issues and hacking threats. He offered the assistance of his association if the committee wished to proceed with further examination.[39]

Laurie Agostinelli, Montana Health Information Management Association, offered to answer any questions and said the association did not think there needed to be any changes to Montana's current law.[40]

Barb Slunaker, health information management, St. Peter's Hospital, agreed with the comments of Mr. Brown and Ms. Agostinelli. She noted that Montana's laws predate HIPAA and said she did not see there would be any benefit in amending the current statutes, but offered her assistance if the committee wished to further examine the area.[41]

In response, to committee member questions, panelists stated that a person is not required to provide a social security number to a health care provider, that written consent is required is most cases, that information security is a constant concern but there was not much that could be done legislatively to help, and that refinements could be made but would require very focused and careful consideration.

[39] State Administration and Veterans' Affairs Interim Committee, Minutes, Montana Legislative Services Division, April 19, 2016, audio/video time 03:13:21.

[40] Ibid., audio/video time 03:16:02.

[41] Ibid., audio/video time 03:16:50.

Discussion and Action

Committee members noted that this was a complex area of law and that working on these matters could perhaps best be done by individual legislators working with specific stakeholders.

Sen. Dee Brown moved that the committee not further examine this area. The motion passed unanimously on a voice vote with Sen. Windy Boy excused.

Government Information

Research

With respect to government information, the committee chose to further examine:

- Whether some state agencies are exempt from following the information management guidelines developed by the state Information Technology Services Division.
- Whether there are penalties if a state agency violates the guidelines.
- Title 50, chapter 16, part 6, MCA, concerning government health care information and consider amendments to clarify that state agencies must still comply with HIPAA. (This issue was handled under the committee's activities related to health information.)

A staff research paper presented on April 19, 2016, covered Montana's current laws with respect to government information technology.[42] Highlights of the report included the following in response to the committee's information requests:

[42] Sheri S. Scurr, "Issue Brief #5 - Government Information: Exceptions to the Montana Information Technology Act" for the State Administration and Veterans' Affairs Interim Committee, Montana Legislative Services Division, April 19, 2016. Also available online by navigating to the committee's website from www.leg.mt.gov.

- The Montana Information Technology Act (SB 131 in 2001) requires statewide IT standards and policies and a strategic IT plan. Part of the purpose of the act is to "protect individual privacy and the privacy of information contained within information technology systems as they become more interconnected". Exceptions are granted under the act as follows:
  - Case-by-case exceptions may be granted to a state agency under section 2-17-515, MCA, if it is "in the best interests of the state of Montana".

  - Specific exceptions for the University System, the Office of Public Instruction, the Montana National Guard, and the Criminal Justice Information Network under section 2-17-516, MCA, which are to accommodate specialized computer systems.

  - A blanket exception for the legislative and judicial branches.

- Montana's Government Internet Information Privacy Act (sections 2-17-550 through 2-17-553, MCA) requires all government websites that collect personally identifiable information to comply with certain requirements. There are no exceptions to these provisions and they cover the state and "political subdivisions of the state". The full text of the main statute of the act is as follows:

2-17-552. Collection of personally identifiable information -- requirements. (1) A government website operator may not collect personally identifiable information online from a website user unless the operator complies with the provisions of this section.

(2) A government website operator shall ensure that the website:

(a) identifies who operates the website;

(b) provides the address and telephone number at which the operator may be contacted as well as an electronic means for contacting the operator; and

(c) generally describes the operator's information practices, including policies to protect the privacy of the user and the steps

taken to protect the security of the collected information.

(3) In addition to the requirements of subsection (2), if the personally identifiable information may be used for a purpose other than the express purpose of the website or may be given or sold to a third party, except as required by law, then the operator shall ensure that the website includes:

(a) a clear and conspicuous notice to the user that the information collected could be used for other than the purposes of the website;

(b) a general description of the types of third parties that may obtain the information; and

(c) a clear, conspicuous, and easily understood online procedure requiring an affirmative expression of the user's permission before the information is collected.

- There are no specific penalties imposed on government entities that violate these provisions because compliance is typically determined through financial and performance audits that are then reported to governing bodies. With respect to state agencies, legislative audits are reported to the Legislative Audit Committee and the full Legislature.

Testimony

Lynne Pizzini, deputy chief information officer and chief information security officer, State Information Technology Services Division (SITSD), Department of Administration, testified that privacy policies are required on the state of Montana website and also for local governments. In responding to questions, Ms. Pizzini said that there is a template available for local governments and she would be the contact for any questions or help that local governments may need in making sure they post privacy policies.[43]

Discussion and Action

[43] State Administration and Veterans' Affairs Interim Committee, Minutes, Montana Legislative Services Division, April 19, 2016, audio/video time 04:51:54.

Committee members discussed whether the committee should focus on government privacy policies to get those in order before focusing on privacy policies in the private sector. Other discussion reflected confidence in the current laws for government information and that the original concern of HJR 21 was to focus on the collecting and selling of consumer information by businesses and the need to provide consumers with more notice and control about how their information is used and distributed to third parties. Further discussion related to the challenges of regulating the worldwide Web and global business practices, but the possibility that the committee might still be able to address consumer rights for Montana consumers with respect to their personal information collected by businesses in Montana. [44]

Sen. Dee Brown moved that the committee request that the SITSD and local government associations engage in an educational process so that all state agencies and political subdivisions come into compliance with current law with respect to posting online privacy policies on the home pages of their websites and that the SITSD take the lead in this educational process.

The motion was amended to include that the SITSD report back to the committee. The motion passed unanimously on a voice vote with Sen. Windy Boy excused.[45]

Shantil Siaperas, Montana Association of Counties (MACo), testified that MACo would carry the message to the counties. Also, a committee letter was sent to MACo and the Montana League of Cities and Towns requesting their attention to the current law requirements concerning privacy policies.

[44] Ibid., audio/video time 04:56:42.

[45] Ibid., audio/video time 05:15:49.

Chapter 2 -
Veteran Suicide Prevention

Recommendations:

LC 1031	A bill revising the state suicide prevention program by further articulating that the program reach all ethnic groups and occupations, that the public awareness campaign be aimed at normalizing the need for all Montanans to address mental health problems, that media outreach include digital and social media, and specifying that veteran groups be solicited to provide input to the public awareness campaign. The bill also provides a $500,000 general fund appropriation (as a starting point for further discussion during the session) to enhance the program.
LC 1030	A bill providing a general fund appropriation of $500,000 (as a starting point for further discussion during the session) for grants through the state suicide prevention office to local efforts targeted at veteran suicide prevention.
LC 1029	A bill requiring that specified health and mental health care professions licensed in Montana complete suicide assessment, treatment, and management training.

Issue Background

Veteran suicide prevention emerged during the later half of the interim as an issue of key concern to committee members. The suicide rate of military veterans residing in Montana is among the highest in the nation.

According to information compiled by the state suicide prevention coordinator:

- For all age groups, Montana has ranked in the top five for suicide rates in the nation, for the past 30 years. In a report for 2014 in the National Vital Statistics Report, Montana has the highest rate of suicide in the nation (251 suicides for a crude rate of 24.5 per 100,000).[46]

- The highest rate of suicide is among American Indians (28 per 100,000) although they only constitute 6% of the state's population.[47]

- Of the 555 Montana suicides between January 2014 and March 2016, 433 (22 percent) were by veterans.[48]

Committee Meetings

Meeting Date	Agenda Items/Information Presented
April 19, 2016	• Staff research memorandum - Info. from Karl Rosston, Suicide Prevention Coordinator, DPHHS • Suicide in Montana, January 2016 - Karl Rosston • Montana Suicide Mortality Review Team Report, January through December 2014

[46] Karl Rosston, "Suicide in Montana: Facts, Figures, and Formulas for Prevention", Montana Department of Public Health and Human Services, January 2016, p. 3. This report is posted on the committee's meeting materials web page for April 19, 2016, which may be accessed by navigating from www.leg.mt.gov.

[47] Ibid., p. 3.

[48] Karl Rosston, "Montana Strategic Suicide Prevention Plan 2017," Montana Department of Public Health and Human Services, p. 20.

Meeting Date	Agenda Items/Information Presented
June 8, 2016	Presentations by and panel discussion with: • Karl Rosston, Suicide Prevention Coordinator • Juliana Hallows, Suicide Prevention Program, VA • Jackie Fitzgerald, Executive Director, Voices of Hope • Meghan Gallagher, Behavioral Health Unit, St. Peter's Hospital • Ed Lesofski, Executive Director, Rural Institute Veterans Education and Research (RIVER) • Brandy Keely, Co-Chair, Lewis and Clark County Joining Community Forces Coalition
Aug. 23, 2016	Presentations and panel discussion on: • Montana Suicide Mortality Review Team recommendations • Joining Community Forces - Community Tool Kit • Suicide Prevention in Indian Country • Overview of Network of Care website • Congressional Efforts and Veterans' Crisis Line • Montana National Guard Suicide Prevention Program Participants included: • Ann Denny, Director, Rocky Boy Veterans Center • Chauncey Parker, American Legion Post 67 Commander, Rocky Boy's Indian Reservation • Juliana Hallows, Suicide Prevention Program, VA • Ed Lesofski, Executive Director, RIVER • Brandy Keely, Lewis & Clark County JCF Co-Chair • Carrie Lutkehus, Community Resources Manager, DPHHS • Mary Lynne Billy-Old Coyote, DPHHS • Jason Smith, State Director of Indian Affairs • BG Ireland, Montana National Guard
Nov. 17, 2016	Discussion and public testimony on preliminary bill drafts: LCvet1 revise state suicide prevention program and provide and appropriation LCvet2 provide an appropriation for grants to local veteran suicide prevention efforts LCvet3 require that certain health professionals receive suicide prevention training

Discussion and Action

Aug. 23, 2016

The committee discussed the recommendations contained in the 2016 Montana Suicide Mortality Review Team report and other recommendations offered by stakeholders during the panel discussion. The main themes discussed were the following:

- Mandatory suicide prevention training and suicide risk assessment training for primary care providers.

- Adding a state American Indian suicide prevention coordinator to the current one-person staff of the state's suicide prevention office.

- Renewal of the statutes (which terminated on June 30, 2016) that established the Montana Suicide Mortality Review Team and statutory updates that would enhance data collection and sharing from tribes, hospitals, and universities.

- A statewide campaign to help normalize conversations about mental health and acknowledge that everyone struggles with stress and that we should talk about depression and anxiety just as we would talk about any physical disease or disability.

- How best to support local approaches to suicide prevention efforts, especially for veterans and American Indians.

During its work session, the committee voted to request three bill drafts for further consideration:

- Support a statewide universal suicide prevention campaign (i.e., a campaign aimed at all demographic groups) with the goal of normalizing our perception of mental health issues and that would use digital technologies.
- Provide state funding for a grant program to help foster local American Indian and veteran suicide prevention efforts.

- Require that primary care physicians receive suicide prevention and risk assessment training.

Nov. 17, 2016

At its final meeting on Nov. 17, 2016, the committee heard public comment, discussed, and took action on each of the preliminary bill drafts related to suicide prevention, as summarized below.

LCvet1 Revise state suicide prevention program (LC 1031)

Proponents included the following individuals:

- Juliana Hallows, suicide prevention coordinator, U.S. Department of Veterans Affairs (VA)
- William Gallea, President, Montana Medical Association (MMA)
- Ed Lesofski, Executive Director, Rural Institute Veterans Education Research (RIVER)

Opponents: none

LCvet2 Fund grants to local veteran suicide prevention efforts (LC 1030)

Proponents included the following individuals:

- Juliana Hallows, suicide prevention coordinator, VA
- William Gallea, President, Montana Medical Association
- Ed Lesofski, Executive Director, RIVER

Opponents: none

LCvet3 Require that certain health professionals receive suicide prevention training (LC 1031)

Proponents included the following individuals:

- Juliana Hallows, suicide prevention coordinator, VA
- Ed Lesofski, Executive Director, RIVER

Opponents included the following individuals:

- William Gallea, President, MMA
- Jean Branscum, MMA

The minutes log of the meeting is available on the committee's Nov. 17, 2016, web page. The audio/video archive of the meeting is available on the committee's homepage.

Appendix A - HJR 21

64th Legislature HJ0021

A JOINT RESOLUTION OF THE SENATE AND THE HOUSE OF REPRESENTATIVES OF THE STATE OF MONTANA REQUESTING AN INTERIM STUDY OF OPPORTUNITIES TO EXPAND OWNERSHIP OF PERSONAL INFORMATION; AND REQUIRING THAT THE FINAL RESULTS OF THE STUDY BE REPORTED TO THE 65TH LEGISLATURE.

WHEREAS, we live in an increasingly digitized age, which allows for personal information to be collected frequently by governmental and corporate entities and then shared, distributed, and sold; and

WHEREAS, collecting and sharing such information increases the potential for such data to be used in a manner not approved of by the owner of that information; and

WHEREAS, there are both benefits and strong privacy concerns that come with this heightened level of data collection, necessitating action to ensure that individuals are able to exert more control over their personal information; and

WHEREAS, there is currently no definitive statute that provides a comprehensive definition of personal information in the technology age; and

WHEREAS, there is confusion as to who owns which pieces of collected personal information and the level of control they may exert over that information; and

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.

NOW, THEREFORE, BE IT RESOLVED BY THE SENATE AND THE HOUSE OF REPRESENTATIVES OF THE STATE OF MONTANA:

That the Legislative Council be requested to designate an appropriate interim committee, pursuant to section 5-5-217, MCA, to study opportunities to expand ownership of personal information.

BE IT FURTHER RESOLVED, that the study:

(1) explore opportunities to provide greater power and control to people regarding information collected about them;

(2) 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;

(3) find methods for consumers to exclude their personal information property from use without severely inhibiting private sector and government functions; and

(4) address, at a minimum, the following types of personal information:

(a) medical records, including records of health conditions, symptoms, treatment, diagnoses, laboratory test information and results, and any information derived from this information;

(b) prescription information, including drug names, dosage, frequency, amounts, dates and times of pickup, and any information derived from this information;

(c) shopping and purchase records, including descriptions of items purchased, the location of purchases, the dates and times of purchases, the price and amounts of purchases, any product return dates, times, locations, and other derived information, and ammunition purchase records, including caliber, brand, price, and amount;

(d) the individual's location, obtained using a handheld communications device carried by the individual, a GPS tracking device, a radio tracking device, a radio frequency identification tag, an automated license plate reader, or facial recognition software;

(e) social security number, driver's license number, state identification card number, or tribal identification card number;

(f) web search terms, browser history, and information derived from this information; and

(g) passwords for personal e-mail, internet, and application accounts not including cryptographic hashes of passwords, such as those commonly used for login authentication.

BE IT FURTHER RESOLVED, that all aspects of the study, including presentation and review requirements, be concluded prior to September 15, 2016.

BE IT FURTHER RESOLVED, that the final results of the study, including any findings, conclusions, comments, or recommendations of the appropriate committee, be reported to the 65th Legislature.

- END -

Appendix B
Glossary of Internet Terms

(Note: The source use for the definition is identified in parentheses following the definition.)

Add-on, Plug-in, or Add-in - A software product designed to enhance another software product. It usually cannot be run independently. (multiple)

Adware - Software that performs certain functions for advertisers, such as sending an ad to a specific website when it is being visited by the consumer that is being tracked by the adware. Adware may be installed on a computer as part of a bundle of software that a consumer purchases, or it may be embedded into a free download. (multiple)

Analytics - The discovery, interpretation, and communication of meaningful patterns in data. Especially valuable in areas rich with recorded information, analytics relies on the simultaneous application of statistics, computer programming, and operations research to quantify performance. Firms may apply analytics to business data to describe, predict, and improve business performance. (Wikipedia)

App - A Web application (Web app) is an application program that is stored on a remote server and delivered over the Internet through a browser interface. (TechTarget)

Algorithm - In mathematics and computer science, an algorithm (e.g., Listeni/'ælg?r?ð?m/ AL-g?-ri-dh?m) is a self-contained step-by-step set of operational instructions to perform a calculation, data processing, and automated reasoning. A computer algorithm is basically an instance of logic written in software by software developers to be effective for the intended "target" computer to produce output from given input. (Wikipedia) Algorithms are used by the behavioral advertising industry to profile consumers.

Beacon or Web Beacon - Also known as a bug, pixel tag, or clear GIF. A clear graphic image (typically one pixel in size) that is delivered through a browser or HTML e-mail. It records an end user's visit to a particular web page or viewing of a particular e-mail. Often used in conjunction with a cookie and used to provide for third-party tracking. Allows specific profiles to be made of user online behavior in combination with web server logs. Certain beacons can report to the sender about which e-mails are read by recipients. Privacy considerations for web beacons are similar to those for cookies. Invisible to the end user. (International Association of Privacy Professionals - IAPP)

Behavioral Advertising - The act of tracking users' online activities and then delivering ads or recommendations based upon the tracked activities. (IAPP)

Breach - The unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a data collector. (IAPP)

Browser - Software program that allows a person to search for and view various kinds of information on the Web. For example, Internet Explorer, Google Chrome, Yahoo!, Bing, and Firefox. (About.com)

Caching - The saving of local copies of downloaded content, reducing the need to repeatedly download content. To protect privacy, pages that display personal information should be set to prohibit caching. (IAPP)

Cloud - Software and services that run on the Internet instead of your computer, for example, Apple iCloud, Dropbox, Netflix, Amazon Cloud Drive, Flickr, Google Drive, Microsoft Office 365, Yahoo Mail. (CNN Money) When something is in the cloud, it means it is stored on servers on the Internet instead of on your computer. It lets you access your calendar, email, files, and more from any computer that has an Internet connection. (GCF LearnFree.org)

Cookie - Small text file stored on a client machine that may later be retrieved by a web server from the machine. Cookies allow web servers to keep track of the end user's browser activities and connect individual web requests into a session. Also used to prevent users from having to be authorized for every password

protected page they access during a session by recording that they have already successfully supplied their user name and password. May be referred to as "first-party" cookeis (if they are placed by the website that is visited) or "third-party" cookies (if they are placed by a party other than the visited website). Additionally, they may be referred to as "session cookies" if they are deleted when a session ends, or "persistent cookies" if they remain longer. (IAPP)

Cross-site Scripting - Code injected by malicious web users into web pages viewed by other users. (IAPP)

Cryptography - The science or practice of hiding information, usually through its transformation. Common cryptographic functions include: encryption, decryption, digital signature and non-repudiation. (IAPP)

Data Matching - An activity that involves comparing personal data obtained from a variety of sources, including "personal information banks", for the purpose of making decisions about the individuals to whom the data pertains. (IAPP)

Deidentification - An action that one takes to remove identifying characteristics from data. De-identified data is information that does not actually identify an individual. (IAPP)

Digital Fingerprinting - The use of web log files to identify a website visitor. Often used for security and system maintenance purposes. Log files generally include: the IP address of the visitor; a time stamp; the URL of the requested page or file; a referrer URL, and the visitor's web browser, operating system and font preferences. In some cases, combining this information can be used to "fingerprint" a device. (IAPP)

Encryption - The process of obscuring information, often through the use of a cryptographic scheme in order to make the information unreadable without special knowledge; i.e., the use of code keys. (IAPP)

Firewall - A network security system, either hardware- or software-based, that controls incoming and outgoing network traffic based on a set of rules. (TechTarget)

Hacker - A person who uses computers to gain unauthorized access to data. (Google online dictionary)

HTML - Hypertext Markup Language. A content authoring language used to create web pages. Browsers use HTML to interpret and render visible and audible content on web pages. Document "tags" can be used to format and lay out web page content and to "hyperlink"—connect dynamically—to other web content. (IAPP)

http - Hypertext Transfer Protocol. A networking language that manages data packets over the Internet. It defines how messages are formatted and transmitted and defines what actions servers and browsers take in response to various commands. (IAPP)

https - Hypertext Transfer Protocol Secure. A secure network communication method, technically not a protocol in itself. HTTPS is the result of layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications. (IAPP)

Hyperlink - Linked graphic or text that is used to connect an end user to other websites, parts of websites or web-enabled services. The URL of a web location is embedded in the HTML code so that when certain words or images are selected through the web browser, the end user is transported to the destination website or page. (IAPP)

Internet - The global system of interconnected mainframe, personal, and wireless computer networks that use the Internet protocol suite (TCP/IP) to link billions of electronic devices worldwide. (Wikipedia)

Intrusion Detection System - IDS. A system that inspects network activity and identifies suspicious patterns that maybe someone is attempting to penetrate or compromise a system or network. An IDS may be network-based or host-based, signature-base or anomaly-based, and requires human intervention in order to respond to the attack. (IAPP)

Intrusion Prevention System (IPS) - A form of access control. An IPS is much like an application firewall. Its intent is not only to detect a network attack but to prevent it. It neither requires nor involves human intervention in order to respond to a system attack. (IAPP)

IP Address - Internet Protocol Address. A unique string of numbers that identifies a computer on the Internet or network. The IP address is expressed in four groups of up to three numbers, separated by periods. For example: 123.123.23.2. May be "dynamic," meaning that it is assigned temporarily whenever a device logs on to a network and so it changes each time a device connects. Or, may be "static," meaning that it is assigned to a particular device and does not change, but remains assigned to one computer or device. (IAPP)

Javascript - A computer scripting language used to produce interactive and dynamic web content. (IAPP)

Location-Based Service - Services that utilize information about location to deliver, in various contexts, a wide array of applications and services, including social networking, gaming and entertainment. Used to identify the real-world geographic location of computer, cell phone, or other device. (IAPP)

Malware - Unwanted or maliciously installed software. A computer virus is a type of malware that replicates itself and spreads within the user's computer like an infection. (multiple)

Opt-In - One of two central concepts of choice. It means an individual makes an active affirmative indication of choice, e.g., checking a box to signal consent share information with third parties. (IAPP)

Opt-Out - One of two central concepts of choice. It means that an individual's lack of action implies that a choice has been made, i.e., unless an individual checks or unchecks a box, his or her information will be shared with third parties. (IAPP)

Passive Data Collection - Data collection in which information is gathered automatically—often without the end user's knowledge—as the user navigates from page to page on a website. This is typically accomplished through the use of cookies, beacons, or other types of identification mechanisms. (IAPP)

Personal Information or Personal Identifying Information (PII) - Any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly—in particular by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity. (IAPP)

Personal Information Banks (PIBs) - Personal information that is organized or intended to be retrievable by a person's name or by a number, symbol, or other identifier assigned only to that person. (multiple)

Phishing - E-mails or other communications that are designed to trick a user into believing that he or she should provide a password, account number or other information. The user then typically provides that information to a website controlled by the attacker. "Spear phishing" is a phishing attack that is tailored to the individual user, such as when an e-mail appears to be from someone the user knows and that instructs the user to provide information. (IAPP)

Pixel tag - See Beacon.

Reidentification - The process of using publicly available information to re-associate personally identifying information with data that has been anonymized. (IAPP)

SSL - See TSL/SSL.

Server Log - Information automatically recorded by a data server when a website is visited. Typically include a users web request, Internet Protocol address, browser type, browser language, the date and time of the request and one or more cookies that may uniquely identify the user's browser. (Wikipedia)

Software - Organized computer program information, such as operating systems,

utilities, and applications that enable computers to work. Consists of instructions and code written by programmers in any of various special computer languages. Commonly divided into two main categories: (1) system software, which is invisible to the user and controls the basic functions of a computer and is usually preinstalled with the machine; and (2) application software, which handles common and specialized tasks that a user wants to perform, such as accounting, communicating, data processing, word processing. (BusinessDictionary.com)

SPAM - Unsolicited commercial e-mail. (IAPP)

Spyware - A type of software that gathers personal information without the individual's knowledge or consent. Some spyware asserts control over a computer without the consumer's knowledge. (multiple)

TLS/SSL - Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL). Cryptographic protocols designed to provide communications security over a computer network. (Wikipedia)

Syndicated Content - The process of pushing content out and onto third-party websites, either as a full article, snippet, link, or thumbnail. (multiple)

Transmission Control Protocol (TCP)- Code that enables two devices to establish a connection and exchange data. (IAPP)

Trojan Horse - A form of malware in which the software masquerades as beneficial software. (IAPP)

Virus - A piece of computer code that is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data. (multiple)

Web or World Wide Web (www) - A system of Internet servers that supports specially formatted documents. The documents are formatted in a markup language called HTML (HyperText Markup Language) that supports links to other documents (i.e, web page), as well as graphics, audio, and video files. Not all Internet servers are part of the Web. (webopedia)

Worm - A type of computer virus that is a program or algorithm that replicates itself over a computer network, usually performing malicious actions. (IAPP)

Links to online glossaries

- Ghostery website - https://www.ghostery.com/intelligence/glossary/

Appendix C
Glossary of Privacy Regulation Terms

(Note: The source for the definition is identified in parentheses following the definition.)

* IAPP is the International Association of Privacy Professionals

Adverse Action
Under the Fair Credit Reporting Act, the term "adverse action" is defined very broadly to include all business, credit and employment actions affecting consumers that can be considered to have a negative impact, such as denying or canceling credit or insurance, or denying employment or promotion. No adverse action occurs in a credit transaction where the creditor makes a counteroffer that is accepted by the consumer. Such an action requires that the decision maker furnish the recipient of the adverse action with a copy of the credit report leading to the adverse action. (IAPP)

APEC Privacy Principles - A set of non-binding principles adopted by the Asia-Pacific Economic Cooperative (APEC) that mirror the OECD Fair Information Privacy Practices. (IAPP)

Article 29 Working Party - A European Union organization that functions as an independent advisory body on data protection and privacy. While EU data protection laws are actually enforced by the national Data Protection Authorities of EU member states. (IAPP)

Binding Corporate Rules - Legally binding internal corporate privacy rules for transferring personal information within a corporate group. BCRs are typically used by corporations that operate in multiple jurisdictions, and they are alternatives to the U.S.-EU Safe Harbor and Model Contract Clauses. BCRs must be approved by the EU data protection authorities of the member states in which the corporation operates. (IAPP)

Binding Safe Processor Rules - Self-regulatory principles (similar to Binding Corporate Rules) for processors that are applicable to customer personal data. Once a supplier's BSPR are approved, a supplier gains "safe processor" status and its customers would be able to meet the EU Data Protection Directive's requirements for international transfers in a similar manner as BCR allow. BSPR are currently being considered as a concept by the Article 29 Working Party and national authorities. (IAPP)

California Investigative Consumer Reporting Agencies Act - A California state law that requires employers to notify applicants and employees of their intention to obtain and use a consumer report. (IAPP)

Canadian Standards Association - A non-profit standards organization that developed its own set of privacy principles and broke the OECD's code into ten principles: (1) Accountability; (2) Identifying purposes; (3) Consent; (4) Limiting Collection; (5) Limiting Use, Disclosure, and Retention; (6) Accuracy; (7) Safeguards; (8) Openness; (9) Individual Access; (10) Challenging Compliance. These ten principles would go on to be listed in PIPEDA. (IAPP)

Charter of Fundamental Rights - A treaty that consolidates human rights within the EU. The treaty states that everyone has a right to protect their personal data, that data must be processed for legitimate and specified purposes and that compliance is subject to control by an authority. (IAPP)

Children's Online Privacy Protection Act of 2000, The - (COPPA). A U.S. federal law that applies to the operators of commercial websites and online services that are directed to children under the age of 13. It also applies to general audience websites and online services that have actual knowledge that they are collecting personal information from children under the age of 13. COPPA requires these website operators: to post a privacy policy on the homepage of the website; provide notice about collection practices to parents; obtain verifiable parental consent before collecting personal information from children; give parents a choice as to whether their child's personal information will be disclosed to third parties; provide parents access and the opportunity to delete the child's personal information and opt out of future collection or use of the

information, and maintain the confidentiality, security and integrity of personal information collected from children. (IAPP)

Confirmed Opt In - An e-mail approach where e-mail marketers send a confirmation e-mail requiring a response from the subscriber before the subscriber receives the actual marketing e-mail. (IAPP)

Consumer Reporting Agency - Any person or entity that complies or evaluates personal information for the purpose of furnishing consumer reports to third parties for a fee. (IAPP)

Cookie Directive - Related to the EU-U.S. Safe Harbor and subsequent Privacy Shield framework. Refers to an EU e-Privacy Directive where websites could allow users to opt out of cookies, such as by selecting a setting on their web browsers. Under the revision, member states are required to pass legislation that gives users the ability to opt in before cookies are placed on their computers. (IAPP)

COPPA Rule - An FTC rule that requires websites and apps to get parental consent before collecting personal information from kids under 13. The Rule was revised in 2013 to strengthen kids' privacy protections and gives parents greater control over the personal information that websites and online services may collect from children under 13. (FTC)

Council of the European Union - The main decision-making body of the EU, it has a central role in both political and legislative decisions. The council was established by the treaties of the 1950s, which laid the foundations for the EU. (IAPP)

Court of Justice of the European Union - The Court of Justice is the judicial body of the EU that makes decisions on issues of EU law and enforces European decisions either in respect to actions taken by the European Commission against a member state or actions taken by individuals to enforce their rights under EU law. The court is the judicial body of the EU that makes decisions on issues of EU law and enforces European decisions. Based in Luxembourg, the Court was set up in 1951, and was originally named the Court of Justice of the European

Communities. The court is frequently confused with the ECHR, which oversees human rights laws across Europe, including in many non-EU countries, and is not linked to the EU institutions. (IAPP)

CSA Privacy Principles - The Canadian Standards Association (CSA) ten privacy principles are based on the OECD Guidelines and serve as the basis of Canada's PIPEDA. (IAPP)

Deceptive Trade Practices - In the context of U.S. federal law, a term associated with corporate entities who mislead or misrepresent products or services to consumers and customers. These practices are regulated in the U.S. by the Federal Trade Commission at the federal level and typically by an attorney general or office of consumer protection at the state level. Law typically provides for both enforcement by the government to stop the practice and individual actions for damages brought by consumers who are hurt by the practices. (IAPP)

Disposal Rule - An FTC rule under the Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), which amended the Fair Credit Reporting Act (FCRA), requires that companies dispose of credit reports and information derived from them in a safe and secure manner. (IAPP)

Do Not Track - A proposed regulatory policy, similar to the existing Do Not Call Registry in the United States, which would allow consumers to opt out of web-usage tracking. (IAPP)

E-Government Act - A U.S. federal law that, among other things, requires federal agencies to conduct Privacy Impact Assessments on new or substantially revised information technology. (IAPP)

Electronic Communications Privacy Act of 1986 - The collective name of the U.S. Electronic Communications Privacy and Stored Wire Electronic Communications Acts, which updated the Federal Wiretap Act of 1968. ECPA, as amended, protects wire, oral and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The act applies to e-mail, telephone conversations and data stored electronically. The USA PATRIOT Act and subsequent federal enactments have clarified and updated

ECPA in light of the ongoing development of modern communications technologies and methods, including easing restrictions on law enforcement access to stored communications in some cases. (IAPP)

European Commission - The executive body of the European Union. Its main function is to implement the EU's decisions and policies, along with other functions. It is also responsible for making adequacy determinations with regard to data transfers to third-party countries. (IAPP)

European Council - A forum where heads of state meet four times a year to define priorities and set political direction for the EU. (IAPP)

European Parliament - The only EU institution whose members are directly elected by member states, Parliament has four responsibilities—legislative development, supervisory oversight of other institutions, democratic representation and budget development. (IAPP)

European Union - The European Union (EU) is comprised of 27 member states including Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden and the United Kingdom. Candidates include Croatia, the Former Yugoslav Republic of Macedonia, Iceland, Montenegro, Serbia and Turkey. (IAPP)

Fair Information Practice Principles - The U.S. Federal Trade Commission Information Practice Principles (FIPP). Guidelines that represent widely accepted concepts and standards concerning fair information practices in an electronic market Place. (Wikipedia) The principles are:

- Transparency: Organizations should be transparent and notify individuals regarding collection, use, dissemination, and maintenance of personally identifiable information (PII).

- Individual Participation: Organizations should involve the individual in the process of using PII and, to the extent practicable, seek individual consent for the collection, use, dissemination, and maintenance of PII. Organizations should also provide mechanisms for appropriate

access, correction, and redress regarding use of PII.

- Purpose Specification: Organizations should specifically articulate the authority that permits the collection of PII and specifically articulate the purpose or purposes for which the PII is intended to be used.
- Data Minimization: Organizations should only collect PII that is directly relevant and necessary to accomplish the specified purpose(s) and only retain PII for as long as is necessary to fulfill the specified purpose(s).

- Use Limitation: Organizations should use PII solely for the purpose(s) specified in the notice. Sharing PII should be for a purpose compatible with the purpose for which the PII was collected.

- Data Quality and Integrity: Organizations should, to the extent practicable, ensure that PII is accurate, relevant, timely, and complete.

- Security: Organizations should protect PII (in all media) through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

- Accountability and Auditing: Organizations should be accountable for complying with these principles, providing training to all employees and contractors who use PII, and auditing the actual use of PII to demonstrate compliance with these principles and all applicable privacy protection requirements. (NSTIC)

Federal Trade Commission (FTC) - An independent U.S. law enforcement agency charged with protecting consumers and enhancing competition across broad sectors of the economy. The FTC's primary legal authority comes from Section 5 of the Federal Trade Commission Act, which prohibits unfair or deceptive practices in the marketplace. The FTC also has authority to enforce a variety of sector specific laws, including the Truth in Lending Act, the CAN-SPAM Act, the Children's Online Privacy Protection Act, the Equal Credit Opportunity Act, the Fair Credit Reporting Act, the Fair Debt Collection Practices Act, and the

Telemarketing and Consumer Fraud and Abuse Prevention Act. This broad authority allows the Commission to address a wide array of practices affecting consumers, including those that emerge with the development of new technologies and business models. (FTC website)

Gramm–Leach–Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999. Requires financial institutions – companies that offer consumers financial products or services like loans, financial or investment advice, or insurance – to explain their information-sharing practices to their customers and to safeguard sensitive data. (FTC website)

Health Breach Notification Rule - An FTC rule that requires certain Web-based businesses to notify consumers when the security of their electronic health information is breached. (FTC website)

National Strategy for Trusted Identities in Cyberspace (NSTIC) - A White House initiative to work collaboratively with the private sector, advocacy groups, public sector agencies, and other organizations to improve the privacy, security, and convenience of online transactions.

Non-Public Personal Information - Defined by U.S. Gramm-Leach-Bliley Act as personally identifiable financial information that is: (i) provided by a consumer to a financial institution, (ii) resulting from a transaction or service performed for the consumer, or (iii) otherwise obtained by the financial institution. Does not include: (i) publicly available information or (ii) any consumer list that is derived without using personally identifiable financial information. (IAPP)

Personal Information or Personal Identifying Information (PII) - Any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly—in particular by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity. (IAPP)

Privacy of Consumer Financial Information Rule. An FTC rule under the GLBA that required financial institutions covered by the Gramm-Leach-Bliley Act must tell their customers about their information-sharing practices and explain to customers their right to "opt out" if they don't want their information shared with certain third parties. (FTC website)

Privacy Rule - Under HIPAA, this rule establishes U.S. national standards to protect individuals' medical records and other personal health information and applies to health plans, healthcare clearinghouses and those healthcare providers that conduct certain healthcare transactions electronically. The rule requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The rule also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records and to request corrections. (IAPP)

Private Right of Action - Unless otherwise restricted by law, any individual that is harmed by a violation of the law can file a lawsuit against the violator. (IAPP)

Privacy Shield - Successor to EU-U.S. Safe Harbor agreement. A mechanism to comply with EU data protection requirements when transferring personal data from the European Union to the United States in support of transatlantic commerce. To join the Privacy Shield Framework, a U.S.-based company will be required to self-certify to the Department of Commerce and publicly commit to comply with the Framework's requirements. While joining the Privacy Shield Framework will be voluntary, once an eligible company makes the public commitment to comply with the Framework's requirements, the commitment will become enforceable under U.S. law. (U.S. Dept. of Commerce website)

Protected Health Information (PHI)- Under U.S. HIPAA law, any information about health status, provision of health care, or payment for health care that is created or collected by a "Covered Entity" (or a Business Associate of a Covered Entity), and can be linked to a specific individual. (Wikipedia)

Red Flags Rule - An FTC rule that requires financial institutions and certain creditors to have identity theft prevention programs to identify, detect, and respond to patterns, practices, or specific activities that could indicate identity theft.

Right To Be Forgotten - A proposed right within the EU, with origins in French law, for individuals to remove information that they had given out about themselves. (IAPP)

Safe Harbor - Recently replaced by the Privacy Shield. The European Commission's (EC) Directive on Data Protection (EC/46/95) prohibits the transfer of personal data to non-European Union nations that do not meet the European "adequacy" standard for privacy protection. While the U.S. and the European Union (EU) share the goal of privacy protection, the U.S. uses a sectoral approach that relies on a mix of legislation, regulation and self-regulation, while the EU relies on comprehensive legislation that requires creation of government data protection agencies, registration of databases with those agencies and, in some instances, approval before personal data processing may begin. As a result of these different privacy approaches, the directive could have significantly hampered the ability of U.S. companies to engage in many trans-Atlantic transactions. In order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the directive, the U.S. Department of Commerce and the EC developed a "Safe Harbor" framework. The Safe Harbor—approved by the EU in 2001—is an important way for U.S. companies to avoid interruptions in business dealings with the EU or prosecution by European authorities under European privacy laws. Certifying to the Safe Harbor assures that EU organizations know a non-EU-based company provides adequate privacy protection, as defined by the directive. From a U.S. perspective, Safe Harbor is a self-regulatory regime that is only available to companies subject to the enforcement authority of the U.S. Federal Trade Commission or the U.S. Department of Transportation. Companies that are outside the jurisdiction of these two agencies are not eligible to join Safe Harbor. (IAPP)

Seal Programs - Programs that require participants to abide by codes of information practices and submit to monitoring to ensure compliance. In return, companies that abide by the terms of the seal program are allowed to display the programs seal on their website. (IAPP)

Sensitive Personal Information - Any information that could be used by criminals to conduct identity theft, blackmail, stalking, or other crimes against an individual.

CI0106 6356shna.