Issue Brief #1

HJR 21 - Study of Personal Information Ownership

For the State Administration and Veterans' Affairs Interim Committee
Prepared by Sheri Scurr, Research Analyst
Montana Legislative Services Division

April 19, 2016

Requiring Notice of Online Information Collection Practices

Purpose and Scope

This issue brief responds to the State Administration and Veterans' Affairs Interim Committee's Feb. 10, 2016, request for further research about requiring websites collecting information on Montana consumers to provide notice of their online information collection practices.

This brief covers:

- The current framework.
- Other states' laws requiring privacy policies or notices.
- Relevant Montana statutes.

Current Framework

EU-U.S. Privacy Shield

The Privacy Shield agreement states:

II. PRINCIPLES

1. NOTICE
   a. An organization must inform individuals about:
      i. its participation in the Privacy Shield and provide a link to, or the web address for, the Privacy Shield List,

      ii. the types of personal data collected and, where applicable, the entities or subsidiaries of the organization also adhering to the Principles,

      iii. its commitment to subject to the Principles all personal data received from the EU in reliance on the Privacy Shield,

      iv. the purposes for which it collects and uses personal information about them,

      v. how to contact the organization with any inquiries or complaints, including any relevant establishment in the EU that can respond to such inquiries or complaints,

      vi. the type or identity of third parties to which it discloses personal information, and the purposes for which it does so,

      vii. the right of individuals to access their personal data,

      viii. the choices and means the organization offers individuals for limiting the use and disclosure of their personal data,

ix. the independent dispute resolution body designated to address complaints and provide appropriate recourse free of charge to the individual ....

x. being subject to the investigatory and enforcement powers of the FTC, the Department of Transportation or any other U.S. authorized statutory body,

xi. the possibility, under certain conditions, for the individual to invoke binding arbitration,

xii. the requirement to disclose personal information in response to lawful requests by public authorities, including to meet national security or law enforcement requirements, and

xiii. its liability in cases of onward transfers to third parties.

b. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party.

Source: Commerce.gov https://www.commerce.gov/privacyshield

Asia-Pacific Economic Cooperation (APEC)

The APEC Privacy Program requires that notifications do the following:

- Provide "clear and easily accessible" statements about the company's personal information policies and practices.
- Describe how personal information is collected.
- Describe the purposes of which personal information is collected.

- Inform consumers about whether their personal information is available to third parties, and if so, for what purposes.

- Provide the company's contact information for questions.

- Provide information about how the consumer may access and correct their personal information.

The APEC program allows for certain exceptions.

Source: Cross Border Privacy Rules Program Requirements
http://www.cbprs.org/GeneralPages/PrivacyinAPECRegion.aspx

Organization for Economic Co-operation and Development (OECD)

Relevant sections of the OECD privacy framework state:

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, ***with the knowledge*** or consent of the data subject.

Purpose Specification Principle

9. The purposes for which personal data are collected ***should be specified not later than at the time of data collection*** and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Openness Principle

12. There should be a ***general policy of openness*** about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Source: The OECD Privacy Framework
http://www.oecd.org/sti/ieconomy/privacy.htm

Federal Trade Commission (FTC)

PROTECTING AMERICA'S CONSUMERS

Notice is one of the Fair Information Practices Principles. The FTC staff's most recent report on "The Internet of Things" recommends:

- Congress should enact baseline privacy standards that include the principle of notice.

- Specific requirements about how notification should be accomplished and technology-specific legislation is not practical or desirable.

Source: FTC staff report, "The Internet of Things: Privacy and Security in a Connected World," January 2015.
https://www.ftc.gov/news-events/press-releases/2015/01/ftc-report-internet-things-urges-companies-adopt-best-practices

Internet Policy Task Force (Dept. of Commerce)

The 2010 task force "green paper" recommendations that could be considered relevant to the principle of notice are as follows:

Recommendation #1:
The Task Force recommends adoption of a baseline commercial data privacy framework built on an expanded set of Fair
Information Practice Principles (FIPPs).

Recommendation #2:
To meet the unique challenges of information intensive environments, FIPPs regarding enhancing transparency, encouraging greater detail in purpose specifications and use limitations, and fostering the development of verifiable evaluation and accountability programs should receive high priority.

Recommendation #3:
Voluntary, enforceable codes of conduct should address emerging technologies and issues not covered by current application of baseline FIPPs. To encourage the development of such codes, the Administration should consider a variety of options, including (a) public statements of Administration support; (b) stepped

up FTC enforcement; and (c) legislation that would create a safe harbor for companies that adhere to appropriate voluntary, enforceable codes of conduct that have been developed through open, multi-stakeholder processes.

Source: Department of Commerce, Internet Policy Task Force, "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework", Dec. 16, 2010.
https://www.ntia.doc.gov/report/2010/commercial-data-privacy-and-innovation-internet-economy-dynamic-policy-framework

Digital Advertising Alliance (DAA)

The DAA's principle related to notice and transparency for is participating companies with respect to data collection for online behavioral advertising states:

II. TRANSPARENCY

A. Third Party and Service Provider Notice

1. Third Party and Service Provider Privacy Notice — Third Parties and Service Providers should give clear, meaningful, and prominent notice on their own Web sites that describes their Online Behavioral Advertising data collection and use practices. Such notice should include clear descriptions of the following:

   (a) The types of data collected online, including any PII for Online Behavioral Advertising purposes;

   (b) The uses of such data, including whether the data will be transferred to a non-Affiliate for Online Behavioral Advertising purposes;

   (c) An easy to use mechanism for exercising choice with respect to the collection and use of the data for Online Behavioral Advertising purposes or to the transfer of such data to a non-Affiliate for such purpose; and

   (d) The fact that the entity adheres to these Principles.

2. Third Party Enhanced Notice to Consumers — In addition to providing notice as described in (1), Third parties should provide enhanced notice as set forth below in (a) or (b):

(a) Third Party Advertisement Notice — Third Parties should provide notice of the collection of data through a clear, meaningful, and prominent link to a disclosure described in II.A.(1):

(i) In or around the advertisement delivered on the Web page where data is collected; or

(ii) On the Web page where the data is collected if there is an arrangement with the First Party for the provision of such notice.

(b) Third Party Participation in Industry-Developed Web Site(s) — Third Parties should be individually listed either:

(i) On an industry-developed Web site(s) linked from the disclosure described in II.B; or

(ii) If agreed to by the First Party, in the disclosure on the Web page where data is collected for Online Behavioral Advertising purposes as described in II.B.

B. Web Site Notice of Third Party Online Behavioral Advertising

When data is collected from or used on a Web site for Online Behavioral Advertising purposes by Third Parties, the operator of the Web site should include a clear, meaningful, and prominent link on the Web page where data is collected or used for such purposes that links to a disclosure that either points to the industry-developed Web site(s) or individually lists such Third Parties. A Web site does not need to include such a link in instances where the Third Party provides notice as described in II.A.(2)(a). A Web site should also indicate adherence to these Principles in its notice.

Source: DAA, "Self-Regulatory Principles for Online Behavioral Advertising", July 2009. http://www.aboutads.info/principles

The NAI code of conduct states:

B. TRANSPARENCY AND NOTICE

1. Each member company shall provide clear, meaningful, and prominent notice on its website that describes its data collection, transfer, and use practices for Interest-Based Advertising and/or Ad Delivery and Reporting. Such notice shall include a general description of the following, as applicable:

    a. The Interest-Based Advertising, and Ad Delivery and Reporting activities undertaken by the member company;

    b. The types of data collected or used for Interest-Based Advertising purposes, and Ad Delivery and Reporting purposes, including any PII;

    c. How such data will be used, including transfer, if any, to a third party;

    d. The technologies used by the member company for Interest-Based Advertising, and Ad Delivery and Reporting; and

    e. The approximate length of time that Interest-Based Advertising or Ad Delivery and Reporting data will be retained by the member company.

    f. A statement that the company is a member of the NAI and adheres to the Code; and

    g. A link to an Opt-Out Mechanism for Interest-Based Advertising.

2. Members that use standard interest segments for Interest-Based Advertising purposes that are based on health-related information or interests shall disclose such segments on their websites.

3. Members shall take steps to require those websites with which they have a contract and engage in Interest-Based Advertising to clearly and conspicuously post notice, which contains:

    a. A statement of the fact that data may be collected for Interest-Based Advertising purposes on the website;

b. A description of the types of data that are collected for Interest-Based Advertising purposes on the website;

c. An explanation of the purposes for which data is collected by, or will be transferred to, third parties; and

d. A conspicuous link to an Opt-Out Mechanism for Interest-Based Advertising.

4. As part of members' overall efforts to promote transparency in the marketplace, members should make reasonable efforts to confirm that websites where the member collects data for Interest-Based Advertising purposes furnish notices comparable to those described in II.B.3 above.

5. Members shall provide, or support the provision or implementation of, notice of Interest-Based Advertising data collection and use practices and the choices available to users, in or around advertisements that are informed by Interest-Based Advertising, unless notice is otherwise provided on the page where the ad is served outside of the publisher's privacy policy or terms of service.

Interactive Advertising Bureau (IAB)

The IAB code of conduct mirrors the DAA code.

Source: IAB Code of Conduct
http://www.iab.com/guidelines/understanding-iab-compliance-programs/

Other States

This section summarizes staff research findings on state statutes requiring notice of privacy policies. The states listed may not be the only states with statutes related to online privacy statements. However, staff reviewed research by the National Conference for State Legislature's on state laws related to Internet Privacy and found that these states were the only ones mentioned whose statutes contained language relevant to this issue brief.

NCSL web page on state laws related to Internet privacy
http://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

California

Online Privacy Protection Act of 2003 - Online Privacy Protection Act of 2003 - California Business and Professions Code sections 22575-22579.
http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=BPC&division=8.&title=&part=&chapter=22.&article=

- Requires operators of commercial web sites or online services that collect personal information on California consumers through a web site to conspicuously post a privacy policy on the site and to comply with its policy.

- The privacy policy must, among other things, identify the categories of personally identifiable information collected about site visitors and the categories of third parties with whom the operator may share the information.

- The privacy policy must also provide information on the operator's online tracking practices.
- An operator is in violation for failure to post a policy within 30 days of being notified of noncompliance, or if the operator either knowingly and willfully or negligently and materially fails to comply with the provisions of its policy.

Source: California's Office of Attorney General web page at
https://oag.ca.gov/privacy/privacy-laws

Connecticut

Connecticut's statute concerning privacy policies is limited to those who collect Social Security numbers.

Gen. Stat. § 42-471 Requiring Privacy Protection Policies
Sec. 42-471. Safeguarding of personal information. Social Security numbers. Privacy protection policy. Civil penalty.
. . . .

(b) Any person who collects Social Security numbers in the course of business shall create a privacy protection policy which shall be published or publicly displayed. For purposes of this subsection, "publicly displayed" includes, but is not limited to, posting on an Internet web page. Such policy shall: (1) Protect the confidentiality of Social Security numbers, (2) prohibit unlawful disclosure of Social Security numbers, and (3) limit access to Social Security numbers.

Source: Connecticut General Assembly web page at
https://www.cga.ct.gov/2011/pub/chap743dd.htm

Delaware

Delaware's statute mirrors California's.

TITLE 6 - Commerce and Trade
SUBTITLE II - Other Laws Relating to Commerce and Trade
CHAPTER 12C. ONLINE AND PERSONAL PRIVACY PROTECTION

§ 1201C Short title.
This chapter shall be known and may be cited as the "Delaware Online Privacy and Protection Act.''

§ 1202C Definitions.
For purposes of this chapter, the following definitions shall apply: …
…

(7) "Conspicuously available'' means, with respect to a privacy policy required by § 1205C of this title, to make the privacy policy available to an individual via the Internet by any of the following means:

a. A webpage on which the actual privacy policy is posted if the webpage is the homepage or first significant page after entering the website.

b. An icon that hyperlinks to a webpage on which the actual privacy policy is posted, if the icon is located on the homepage or the first significant page after entering the website, and if the icon contains the word "privacy.'' The icon shall also use a color that contrasts with the background color of the webpage or is otherwise distinguishable.

c. A text link that hyperlinks to a webpage on which the actual privacy policy is posted, if the text link is located on the homepage or first significant page after entering the website, and if the text link includes the word "privacy,'' is written in capital letters equal to or greater in size than the surrounding text, or is written in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the language.

d. Any other functional hyperlink that is so displayed that a reasonable individual would notice it.

e. With respect to an internet website, online or cloud computing service, online application, or mobile application that is not a website, any other reasonably accessible and visible means of making the privacy policy available for users of the internet website, online or cloud computing service, online application, or mobile application.

§ 1205C Posting of privacy policy by operators of commercial online sites and services.

(a) An operator of a commercial internet website, online or cloud computing service, online application, or mobile application that collects personally identifiable information through the Internet about individual users residing in Delaware who use or visit the operator's commercial internet website, online or cloud computing service, online application, or mobile application shall make its privacy policy conspicuously available on its internet website, online or cloud computing service, online application, or mobile application. An operator shall be in violation of this subsection only if the operator fails to make its privacy policy conspicuously available within 30 days after being notified of noncompliance.

(b) The privacy policy required by subsection (a) of this section shall do all of the following:

(1) Identify the categories of personally identifiable information that the operator collects through the internet website, online or cloud computing service, online application, or mobile application about users of its commercial internet website, online or cloud computing service, online application, or mobile application and the categories of third-party persons with whom the operator may share that personally identifiable information.

(2) If the operator maintains a process for a user of the internet website, online or cloud computing service, online application, or mobile application to review and request changes to any of that user's personally identifiable information that is collected through the internet website, online or cloud computing service, online application, or mobile application, provide a description of that process.

(3) Describe the process by which the operator notifies users of its commercial internet website, online or cloud computing service, online application, or mobile application of material changes to the operator's privacy policy for that internet website, online or cloud computing service, online application, or mobile application.

(4) Identify the effective date of the privacy policy.

(5) Disclose how the operator responds to web browser "do not track'' signals or other mechanisms that provide users the ability to exercise choice regarding the collection of personally identifiable information about a user's online activities over time and across third-party internet websites, online or cloud computing services, online applications, or mobile applications, if the operator engages in that collection.

(6) Disclose whether other parties may collect personally identifiable information about a user's online activities over time and across different internet websites, online or cloud computing services, online applications, or mobile applications when a user uses the operator's internet website, online or cloud computing service, online application, or mobile application.

(7) An operator may satisfy the requirement of paragraph (b)(5) of this section by providing a clear and conspicuous hyperlink in the operator's privacy policy to an online location containing a description, including the effects, of any program or protocol the operator follows that offers the user that choice.

(c) An operator of a commercial internet website, online or cloud computing service, online application, or mobile application that collects personally identifiable information through the internet website, online or cloud computing service, online application, or mobile application from users of its internet website, online or cloud computing service, online application, or mobile application who reside in Delaware shall be in violation of this section if the operator fails to comply with the provisions of this section, rules and regulations promulgated pursuant to subsection (b) of this section, or with the provisions of the operator's posted privacy policy either (i) knowingly and wilfully or (ii) negligently and materially.

§ 1203C Enforcement.
The Consumer Protection Unit of the Department of Justice has enforcement authority over this chapter and may investigate and prosecute violations of this chapter in accordance with the provisions of subchapter II of Chapter 25 of Title 29.

Source: Delaware Code Online
http://delcode.delaware.gov/title6/c012c/index.shtml

Utah

Utah prohibits a commercial entity from selling nonpublic personal information collected from an online consumer transaction unless the entity provides notice to the consumer.

See Utah codes: Title 13, chapter 37 - Notice of Intent to Sell Nonpublic Personal Information Act
http://le.utah.gov/xcode/Title13/Chapter37/13-37.html?v=C13-37_1800010118000101

Montana's Statutes

Montana does not currently require online commercial entities to post a privacy policy. 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 is:

> **30-14-103. Unlawful practices.** Unfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are unlawful.