# DISCLOSURE OF CONSUMERS' PERSONAL DATA - BACKGROUND MEMORANDUM

House Bill No. 1485 (2019) (appendix) directs the Legislative Management to study protections, enforcement, and remedies regarding the disclosure of consumers' personal data. The study must include a review of privacy laws of other states and applicable federal law.

## BILL HISTORY

As introduced, House Bill No. 1485 would have prohibited covered entities from disclosing any part of a record containing an individual's personal information to any person other than the individual who is the subject of the record, without the individual's express written consent. The bill would have authorized the Attorney General to enforce the law by utilizing various powers, including obtaining an injunction, issuing a cease and desist order, or bringing an action in district court to recover penalties. The bill also would have permitted an individual to bring a civil action to recover damages, costs, and fees if a covered entity purchased, received, sold, or shared the individual's personal information in violation of the chapter.

The House Industry, Business and Labor Committee considered an amendment to the bill which would have essentially mirrored a data privacy bill that had been introduced in the Washington State Legislature in January 2019. Ultimately, House Bill No. 1485 was amended to provide for a mandatory Legislative Management study on protections, enforcements, and remedies regarding the disclosure of consumers' personal data, and both chambers passed the bill as a mandatory study.

## BACKGROUND

Security and privacy issues relating to personal data are a growing concern. These issues have become increasingly relevant as the Internet and new technology have made individuals' personal information and data more accessible and easier to collect, access, and repurpose or manipulate. Personal data includes information, such as an individual's email address, phone number, birthdate, Social Security number, or credit card information.

Generally, data privacy involves controlling who has access to individuals' personal information. Data privacy laws include laws requiring organizations to keep individuals' personal information confidential, allowing consumers to opt out of data collection or otherwise control the sharing of their information, and keeping children's personal information private. Data security usually involves protecting individuals' personal information from unauthorized access. Data security laws include laws requiring businesses and government to take specific measures to keep data secure, security breach laws, and other cybersecurity legislation.

Privacy regulation in the United States has focused primarily on protecting particular types of personal information, such as financial or health information. However, recently, there has been a push to regulate privacy more broadly as it relates to individuals' personal information.

The first major advance to regulate the privacy of consumers' personal data occurred in Europe. In May 2018 the European Union's General Data Protection Regulation (GDPR) took effect, extending European Union jurisdiction beyond those countries. Any global business that sells to or has European Union customers is subject to the GDPR, regardless of where the business is based. The GDPR sets forth rules about how companies treat the personal data of European Union citizens, even those purchasing United States products or services or living in the United States. The influence of the rules is most evident in the notifications regarding the use of "cookies" that recently began appearing on websites. A cookie is a small amount of data generated by a website and saved by the web browser which are used by websites for authentication, storing website information and preferences, and other browsing information.

## FEDERAL PRIVACY LAWS

The United States lacks a single, comprehensive federal law that regulates the collection and use of personal information. Since the implementation of the European Union's GDPR and as other states have been introducing legislation addressing data privacy, interest has been developing for a comprehensive federal privacy law. Federal lawmakers have introduced several privacy bills, varying in scope, but no formal action has been taken at this time. Instead, the federal government has primarily addressed privacy and security by regulating only certain sectors and types of sensitive information, such as health and financial information. Although there are privacy provisions in a broad range of federal laws, a few Acts at the forefront of the privacy issue include the Health Insurance Portability and Accountability Act of 1996 (HIPAA); the Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act; the Fair Credit Reporting Act; and the Children's Online Privacy Protection Act.

### Health Insurance Portability and Accountability Act of 1996

The Health Insurance Portability and Accountability Act of 1996 was drafted in part to address the lack of a comprehensive federal law protecting the privacy of individuals' medical records. The privacy regulations issued pursuant to HIPAA outline the allowable uses and disclosures of individuals' protected health information held by covered entities. Protected health information includes any information held by a covered entity regarding health status, provision of health care, or health care payment that can be linked to an individual, and the term has been interpreted to include any part of an individual's medical record or payment history.

The regulations give individuals the right to obtain copies of their health data to check their health records for errors and to share their records with whomever they wish. The regulations apply to health care clearinghouses, health plans, and health care providers that engage in certain transactions. The regulations also apply to personally identifiable information in any form, whether communicated electronically, on paper, or orally.

### Financial Services Modernization Act of 1999 - Gramm-Leach-Bliley Act

The federal Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act, requires financial institutions--companies that offer consumers financial products or services such as loans, financial or investment advice, or insurance--to explain their privacy and information-sharing practices to their customers and to safeguard sensitive data. The Act places limitations on financial institutions' sharing of consumers' nonpublic personal information with nonaffiliated third parties and requires financial institutions to offer consumers the right to opt-out of such sharing.

### Fair Credit Reporting Act

The Fair Credit Reporting Act of 1970 was the first legislation enacted at the federal level to protect privacy by regulating personal recordkeeping practices in the private sector. The purpose of the Act is to promote accuracy and ensure privacy of information used in consumer reports. The Act provides the circumstances under which consumer reports may be furnished, establishes what information can be included in the report, and provides procedures for disclosures and corrections. Under the Act, consumers have a right to view the information in their credit file and to dispute inaccurate information.

### Children's Online Privacy Protection Act

The Children's Online Privacy Protection Act, enacted in October 1998, applies to the online collection of personal information about children under 13 years of age by persons or entities under United States jurisdiction. The Act details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and the responsibilities an operator has to protect children's privacy and safety online including restrictions on the marketing of those under the age of 13.

## NORTH DAKOTA DATA PRIVACY AND SECURITY LAWS

In 2005 legislation was enacted to create North Dakota Century Code Chapter 51-30, regarding security breach notification. Chapter 51-30 requires a person that owns or licenses computerized data that includes personal information to disclose or notify consumers of breaches involving the consumers' personal information. The Attorney General is authorized to enforce the chapter.

During the 2019 legislative session, a bill was introduced to regulate data brokers, which are businesses that collect and sell or license a consumer's personal information to third parties. House Bill No. 1524 would have required data brokers to register with the Secretary of State, pay a registration fee, and develop and maintain a comprehensive information security program to secure individuals' personal information. The bill would have authorized the Attorney General to enforce the new law. The bill was amended by the House to provide for a Legislative Management study on the privacy practices in the data broker industry. The bill failed to pass the Senate, in part due to acknowledgment of the Legislative Management study on the disclosure of consumers' personal data outlined in House Bill No. 1485.

## OTHER STATES' LAWS

In 2018 the stage was set for comprehensive consumer data privacy legislation. As mentioned above, the European Union's GDPR took effect in May 2018. In addition, California enacted one of the broadest online privacy laws in the country in 2018.

California often has led the way in enacting privacy protections for its citizens. In 2002 California enacted some of the first laws requiring notifications of data security breaches, and in 2004, California enacted the first law requiring website privacy policies. As the GDPR began taking effect, advocates in California were gathering signatures for a data privacy measure for the November 2018 ballot. The backers of the initiative agreed to not

place the measure on the ballot after the state legislature introduced a similar proposal, namely the California Consumer Privacy Act of 2018 (CCPA). The Act regulates the collection, use, sale, and disclosure of California residents' personal information by qualifying businesses. The bill was signed into law on June 28, 2018, but will not go into effect until January 1, 2020. The Act is considered the most expansive state privacy law in the United States. The Act:

- Grants consumers the right to request a business to disclose the categories and specific pieces of personal information the business has collected about the consumers, the source of the information, and the business purpose for collecting the information;
- Grants consumers the right to opt-out of a business's sale of their personal information, and provides businesses may not discriminate against consumers who opt-out;
- Allows consumers to request businesses to delete personal information the business has collected from the consumers; and
- Provides for enforcement by the state attorney general and a private right of action in certain cases of unauthorized access, theft, or disclosure of a consumer's personal information.

The California Attorney General will be promulgating regulations to help establish procedures to facilitate consumers' rights under the CCPA and to provide guidance for businesses on how to comply. In addition, the California State Legislature is considering several amendments to the CCPA. The California State Legislature will adjourn its current session by September 13, 2019.

In 2018 Vermont also passed legislation requiring data brokers to disclose to individuals what data is being collected and to permit individuals to opt-out of the collection.

During the 2019 legislative sessions across the country, a significant number of bills addressing data privacy were introduced in numerous states, including the Washington State Legislature bill after which one amendment to North Dakota House Bill No. 1485 (2019) was mirrored. Washington state legislators introduced the Washington Privacy Act (WPA) in January 2019. Unlike other states, such as Hawaii, Maryland, and New Mexico that modeled their bills largely on the CCPA, the WPA established requirements that were more similar to the GDPR. In addition to requirements for notice and consumer rights such as access, correction, and deletion, the WPA imposed restrictions on the use of automatic profiling and facial recognition. The Washington bill passed the Senate; however, the House of Representatives failed to vote on the bill before the legislative deadline.

The National Conference of State Legislatures identified at least 25 states that introduced bills in 2019 to address issues, such as the regulation of privacy practices of commercial entities, online services, or commercial websites; online privacy; the collection of consumers' biometric data, and data broker regulation. The table can be found at http://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.

The National Conference of State Legislatures also has identified at least 25 states with laws that address data security practices of private sector entities. The table can be found at *http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx#DataSecLaws*. Most of these laws require businesses that own, license, or maintain personal information about a resident of the state to implement and maintain "reasonable security procedures and practices" appropriate to the nature of the information and to protect the information from unauthorized access, destruction, use, modification, or disclosure. More than one-half of the states also have enacted data disposal laws requiring entities to destroy or dispose of personal information so the information is unreadable or indecipherable.

## Uniform Law Commission

The Uniform Law Commission (ULC) has recognized data security and privacy as a topic for consideration as a uniform law. The Uniform Law Commission's Study Committee on Data Breach Notification met over the last year to determine whether the topic should be addressed by a drafting committee. The study committee studied the need for and feasibility of state legislation on data breach notification and considered the personal information that should be protected and the methods and manner of notice that should be provided. The committee's final report on its recommendation to proceed with a drafting committee was submitted to the Scope and Program Committee for consideration at the ULC meeting in July 2019 in Anchorage, Alaska. The Executive Committee of the ULC authorized the appointment of the drafting committee on collection and use of personally identifiable data.

## PROPOSED STUDY APPROACH

There are a variety of study approaches the committee may wish to consider. First, the committee may wish to receive testimony from persons interested in consumers' data privacy and security, including the Attorney General and the Department of Commerce, to gain perspective on considerations regarding protections, enforcement, and remedies relating to the disclosure of consumers' personal data, and an update on how, or if, ULC will address the issue.

The gathering of this information may assist the committee in evaluating whether the state should regulate the disclosure of consumers' personal data. Additionally, the committee may wish to consider the positive and negative social and economic impacts such regulation will have on the state. Consideration of the impacts of regulation may lead the committee to consider whether legislation is appropriate. If the committee recommends legislative action, it may be helpful to evaluate actions taken by other states and to research those states' approaches.

ATTACH:1