19.1041.01001

Sixty-sixth
Legislative Assembly
of North Dakota

HOUSE BILL NO. 1524

Introduced by

Representatives Beadle, Bosch, Mock, Toman

Senators Davison, Meyer, Robinson

1   A BILL ~~for an Act to create and enact chapter 51-30.1 of the North Dakota Century Code,~~

2   ~~relating to the regulation of data brokers; and to provide a penalty.~~for an Act to provide for a

3   legislative management study of privacy practices in the data broker industry.

4   **BE IT ENACTED BY THE LEGISLATIVE ASSEMBLY OF NORTH DAKOTA:**

5   **SECTION 1.** ~~Chapter 51-30.1 of the North Dakota Century Code is created and enacted as~~

6   ~~follows:~~

7   ~~**51-30.1-01. Definitions.**~~

8   ~~As used in this chapter:~~

9   ~~1.   "Biometric data" means data generated from measurements or technical analysis of~~

10 ~~human body characteristics used to identify or authenticate the consumer. The term~~

11 ~~includes a fingerprint, retina or iris image, or other unique physical representation or~~

12 ~~digital representation of biometric data.~~

13 ~~2.   "Consumer" means an individual residing in this state.~~

14 ~~3.   "Data broker" means a business, or unit of a business, separately or together, which~~

15 ~~knowingly collects and sells or which licenses to third parties the brokered personal~~

16 ~~information of a consumer with whom the business does not have a direct relationship.~~

17 ~~4.   "Encryption" means use of an algorithmic process to transform data into a form in~~

18 ~~which the data is rendered unreadable or unusable without use of a confidential~~

19 ~~process or key.~~

20 ~~5.   "Personal information" means one or more of the following computerized data~~

21 ~~elements about a consumer, if categorized or organized for dissemination to third~~

22 ~~parties:~~

23 ~~a.   Name;~~

24 ~~b.   Address;~~

1   c.   Date of birth;

2   d.   Place of birth;

3   e.   Mother's maiden name;

4   f.   Unique biometric data;

5   g.   Name or address of a member of the consumer's immediate family or household;

6   h.   Social security number or other government-issued identification number; or

7   i.   Other information that, alone or in combination with the other information sold or

8   licensed, would allow a reasonable person to identify the consumer with

9   reasonable certainty.

10   6.   "Security breach" means unauthorized acquisition of electronic data, or a reasonable

11   belief of an unauthorized acquisition of electronic data, which compromises the

12   security, confidentiality, or integrity of a consumer's personally identifiable information

13   maintained by a data collector.

14 **51-30.1-02. Registration - Penalty.**

15   1.   Annually, before February first following a year in which a person meets the definition

16   of data broker, a data broker shall:

17   a.   Register with the secretary of state;

18   b.   Pay a registration fee of one hundred dollars; and

19   c.   Provide the following information:

20   (1)   The name and primary physical, electronic mail, and internet addresses of

21   the data broker;

22   (2)   If the data broker permits a consumer to opt-out of the data broker's

23   collection of personal information, opt-out of the data broker's databases, or

24   opt out of certain sales of data:

25   (a)   The method for requesting an opt-out;

26   (b)   If the opt-out applies only to certain activities or sales, which activities

27   or sales; and

28   (c)   Whether the data broker permits a consumer to authorize a third party

29   to perform the opt-out on the consumer's behalf;

30   (3)   A statement specifying the data collection, database, or sales activity from

31   which a consumer may not opt-out;

1   (4)   A statement whether the data broker implements a purchaser credentialing

2   process;

3   (5)   The number of data broker security breaches the data broker has

4   experienced during the previous year, and if known, the total number of

5   consumers affected by the breaches;

6   (6)   If the data broker has actual knowledge the data broker possesses the

7   personal information of minors, a separate statement detailing the data

8   collection practice, database, sales activity, and opt-out policy applicable to

9   the personal information of a minor; and

10   (7)   Any additional information or explanation the data broker chooses to provide

11   concerning the data broker's data collection practices.

12   2.   A data broker that fails to register under this subsection is subject to a civil penalty of

13   fifty dollars for each day, not to exceed a total of ten thousand dollars for each year,

14   the data broker fails to register.

15   **51-30.1-03. Comprehensive information security program.**

16   1.   A data broker shall develop, implement, and maintain a comprehensive information

17   security program written in one or more readily accessible parts which contains

18   administrative, technical, and physical safeguards appropriate to the:

19   a.   Size, scope, and type of business of the data broker obligated to safeguard the

20   personal information under the comprehensive information security program;

21   b.   Amount of resources available to the data broker;

22   c.   Amount of stored data; and

23   d.   Need for security and confidentiality of personal information.

24   2.   A data broker shall adopt safeguards in the comprehensive security program which

25   are consistent with the safeguards for protection of personal information and

26   information of a similar character set forth in federal regulations applicable to the data

27   broker.

28   3.   A comprehensive information security program must include:

29   a.   Designation of one or more employees to maintain the program;

30   b.   Identification and assessment of reasonably foreseeable internal and external

31   risks to the security, confidentiality, and integrity of any electronic, paper, or other

1   records containing personal information, and a process for evaluating and

2   improving, as necessary, the effectiveness of the safeguards for limiting the risks,

3   including:

4   (1)   Ongoing employee training, including training for temporary and contract

5   employees;

6   (2)   Employee compliance with policies and procedure requirements; and

7   (3)   Means for detecting and preventing security system failures;

8   c.   Security policies for employees relating to the storage, access, and transportation

9   of records containing personal information outside business premises;

10   d.   Disciplinary measures for violations of the comprehensive information security

11   program rules;

12   e.   Measures to prevent a terminated employee from accessing records containing

13   personal information;

14   f.   Supervision of service providers, by:

15   (1)   Taking reasonable steps to select and retain third-party service providers

16   capable of maintaining appropriate security measures to protect personal

17   information consistent with applicable law; and

18   (2)   Requiring third-party service providers, by contract, to implement and

19   maintain appropriate security measures for personal information;

20   g.   Reasonable restrictions on physical access to records containing personal

21   information and storage of the records and data in a locked facility, storage area,

22   or container;

23   h.   Regular monitoring to ensure the comprehensive information security program is

24   operating in a manner reasonably calculated to prevent unauthorized access to

25   or unauthorized use of personal information and upgrading information

26   safeguards as necessary to limit risks;

27   i.   Regular review of the scope of the security measures at least annually or if there

28   is a material change in business practices which may reasonably implicate the

29   security or integrity of records containing personal information; and

30   j.   Documentation of responsive actions taken in connection with any incident

31   involving a breach of security and mandatory post-incident review of events and

				actions taken, if any, to make changes in business practices relating to protection
1				
2				of personal information.
3	4.			A comprehensive information security program required by this section must have, at
4				minimum and to the extent technically feasible, the following elements:
5		a.		Secure user authentication protocols, as follows:
6			(1)	An authentication protocol that has the following features:
7				(a) Control of user identifications and other identifiers;
8				(b) A reasonably secure method of assigning and selecting passwords or
9				use of unique identifier technologies, such as biometrics or token
10				devices;
11				(c) Control of data security passwords to ensure the passwords are kept
12				in a location and format that do not compromise the security of the
13				data the passwords protect;
14				(d) Restricting access to active users and active user accounts only; and
15				(e) Blocking access to user identification after multiple unsuccessful
16				attempts to gain access; or
17			(2)	An authentication protocol providing a higher level of security than the
18				features specified in paragraph 1.
19		b.		Secure access control measures that:
20			(1)	Restrict access to records and files containing personal information to those
21				who need the information to perform job duties; and
22			(2)	Assign to each individual with computer access unique identifications plus
23				passwords, which are not vendor-supplied default passwords, which are
24				reasonably designed to maintain the integrity of the security of the access
25				controls, or a protocol that provides a higher degree of security;
26		c.		Encryption of all transmitted records and files containing personal information
27				that will travel across public networks and encryption of all data containing
28				personally identifiable information to be transmitted wirelessly, or a protocol that
29				provides a higher degree of security;
30		d.		Reasonable monitoring of systems for unauthorized use of or access to personal
31				information;

1   ~~e.   Encryption of all personal information stored on a laptop or other portable device,~~

2   ~~or a protocol that provides a higher degree of security;~~

3   ~~f.   For files containing personal information on a system connected to the internet,~~

4   ~~reasonably up-to-date firewall protection and operating system security patches~~

5   ~~reasonably designed to maintain the integrity of the personal information, or a~~

6   ~~protocol that provides a higher degree of security;~~

7   ~~g.   Reasonably up-to-date versions of system security agent software that include~~

8   ~~malware protection and reasonably up-to-date patches and virus definitions, or a~~

9   ~~version of the software that can be supported with up-to-date patches and virus~~

10   ~~definitions and is set to receive the most current security updates on a regular~~

11   ~~basis, or a protocol that provides a higher degree of security; and~~

12   ~~h.   Education and training of employees on the proper use of the computer security~~

13   ~~system and the importance of personal information security.~~

14   ~~**51-30.1-04. Enforcement - Powers - Remedies - Penalties.**~~

15   ~~The attorney general may enforce this chapter. The attorney general, in enforcing this~~

16   ~~chapter, has all the powers provided in chapter 51-15 and may seek all the remedies in chapter~~

17   ~~51-15. A violation of this chapter is deemed a violation of chapter 51-15. The remedies, duties,~~

18   ~~prohibitions, and penalties of this chapter are not exclusive and are in addition to all other~~

19   ~~causes of action, remedies, and penalties under chapter 51-15, or otherwise provided by law.~~

20   **SECTION 1. LEGISLATIVE MANAGEMENT STUDY - DATA BROKER INDUSTRY.** During

21   the 2019-20 interim, the legislative management shall consider studying privacy practices in the

22   data broker industry to determine whether adequate safety measures exist to prevent fraud and

23   protect the identifying information of consumers. The study must include consultation with the

24   department of commerce and the attorney general, and an evaluation of the nature and sources

25   of the consumer information the data brokers collect, how data brokers use, maintain, and

26   disseminate the information, and the extent to which the data brokers allow consumers to

27   access and correct their information or to opt out of having their personal information sold. The

28   legislative management shall report its findings and recommendations, together with any

29   legislation required to implement the recommendations, to the sixty-seventh legislative

30   assembly.