Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

Writers email: eellman@cdiaonline.org
Writer's direct dial: +1 (202) 408-7407
CDIAONLINE.ORG

August 20, 2020

The Honorable Jane Nelson
The Honorable Giovanni Capriglione
Co-Chairs, Texas Privacy Protection Advisory Committee
Austin, TX 78678

Dear Chair Nelson and Chair Capriglione:

I write on behalf of the Consumer Data Industry Association ("CDIA") to respond to a Request for Information ("RFI") your committee has proposed on privacy issues. As your committee discusses possible privacy legislation in 2021, we hope that you will keep in mind several core CDIA principles, that any state privacy law should (1) Exempt key existing federal privacy laws; (2) Exempt public records; (3) Allow data use for fraud prevention; and (4) Focus only on consumer information, and not commercial information.

The Consumer Data Industry Association is the voice of the consumer reporting industry, representing consumer reporting agencies, including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs.

1. Any state privacy law should exempt existing federal privacy laws

Privacy in the United States has, as you know, been regulated on a sectorial basis, rather than on a one-size-fits-all basis. Even though there is a long history of sectorial privacy controls, history is changing. California adopted what in many respects is a one-size-fits-all approach to privacy, but with substantial exemptions to recognize a number of long-standing privacy laws. Any Texas privacy bill should allow already regulated sectors to continue to operate under their national privacy controls. To help consumers meet their expectations and to allow businesses to serve those consumers in a fair way, CDIA respectfully requests that any Texas privacy bill exempt the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq.* ("FCRA"), the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801 *et seq.* ("GLBA"), and the Drivers Privacy Protection Act, 18 U.S.C. §§ 2721 *et seq.* ("DPPA").

A. The need for an exemption for the Federal Fair Credit Reporting Act

Any state privacy law should include clear and concise language exempting consumer data already regulated under the FCRA. The FCRA provides important and necessary protections to consumers, lenders, government agencies, law enforcement, volunteer organizations, and businesses who rely on full, complete and accurate consumer reports to meet their needs and expectations and make informed decisions. An incomplete FCRA exemption risks negatively impacting the integrity of the consumer reporting ecosystem, and therefore the safety and soundness of the economy.

To assist your committee, we propose the following FCRA exemption, modeled after the FCRA exemption in both the California Consumer Credit Reporting Act ("CCPA") and the Washington Privacy Act ("WPA")[1]:

> This [act] [title] [chapter] does not apply to an activity involving personal information governed by the Fair Credit Reporting Act, section 1681 *et seq.*, Title 15 of the United States Code, or otherwise used to generate a consumer report, by a consumer reporting agency, as defined by 15 U.S.C. Sec. 1681a(f), by a furnisher of information, or by a person procuring or using a consumer report.[2]

Passed in 1970, the FCRA is the country's first national privacy law. The law has been amended many times over the years to ensure consumer protections are properly maintained as technology and use of consumer data has evolved. The FCRA has long held robust consumer protections including the right:

- To know what information is collected about consumers,
- To know who has accessed consumer information,
- To know if information included in a consumer report results in an adverse action, and
- To correct and delete inaccurate information on a consumer's file.

The FCRA provides for strictly controlled permissible purposes to limit access to consumer reports by data users. The FCRA also affords substantial identity theft prevention and mitigation rights for consumers and duties for businesses. For enforcement purposes, the FCRA provides for private rights of action, and enforcement by state attorneys general, the Consumer Financial Protection Bureau ("CFPB"), and the Federal Trade Commission ("FTC").

---

[1] The WPA passed the Washington Senate with an FCRA exemption and while that exemption was unchanged in the House, the WPA did not pass the House.

[2] The FCRA exemption in the CCPA is long and cumbersome. Cal. Civ. Code § 1785.145(d). Our proposed FCRA exemption is substantively and legally identical to the CCPA, but achieves the same end – no more and no less – in far less words than the CCPA.

The value and purpose of the FCRA was best summed up by former FTC chair, Tim Muris when he said that "[t]he FCRA is an intricate statute that strikes a fine-tuned balance between privacy and the use of consumer information. At its core, it ensures the integrity and accuracy of consumer records and limits the disclosure of such information to entities that have 'permissible purposes' to use the information."[3] Muris referred to the "miracle of instant credit" and the genius of the consumer reporting system. Muris said that "[t]he system works because, without anybody's consent, very sensitive information about a person's credit history is given to the credit reporting agencies. If consent were required, and consumers could decide - on a creditor-by-creditor basis - whether they wanted their information reported, the system would collapse."[4]

A collection of consumer groups called the FCRA "a robust law that gives consumers Fair Information Practices based rights. For example, consumers have the right to know about, inspect, dispute and correct their files. The FCRA requires purpose specificity before a report can be accessed."[5] The FTC called the FCRA "an important tool that provides consumers with the right to access their own data that has been used to make such decisions, and if it is erroneous, to correct it."[6]

The foundation of the American economy is credit. The cornerstone of this credit economy is the credit reporting system, which is made up of consumer reporting agencies. The broad, national consumer reporting ecosystem is governed by the FCRA.

It is the FCRA, and the entities governed by it, that allows consumers to apply for a mortgage at night, from a kitchen table. It is the FCRA that allows consumers to purchase a $30,000 car from someone they just met on a Saturday afternoon. It is the FCRA that allows nonprofits and volunteer groups to conduct background checks on prospective volunteers. It is the FCRA that allows child support enforcement agencies to locate parents who are delinquent on their child support obligations.

If state privacy law was to limit the accuracy, access, or use of consumer information for FCRA purposes, consumers would ultimately be negatively impacted. Consumer information regulated under existing federal statute helps consumers achieve their financial goals, such as

---

[3] FTC Chairman Tim Muris, Oct. 4, 2001 before the Privacy 2001 conference, Cleveland, Ohio ("Muris").
[4] *Id*.
[5] Hearing on *Data Security, Data Breach Notices, Privacy and Identity Theft,* before the Senate Comm. on Banking, Housing, and Urban Affairs, Sept. 22, 2005 (111th Cong.) (statement of Edmund Mierzwinski U.S. PIRG on behalf of Consumer Federation of America, Consumers Union, Electronic Privacy Information Center (EPIC), Privacy Rights Clearinghouse, Privacy Times, U.S. Public Interest Research Group (U.S. PIRG), and World Privacy Forum ("Consumer Groups").
[6] Protecting Consumer Privacy in an Era of Rapid Change, Fed. Trade Comm., March 2012, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

obtaining mortgages and car loans, receiving student aid, opening a checking account and more. Failing to recognize the importance of this well-established federal statute and its existing consumer data protections will result in higher interest rates and limit consumer's access to affordable credit.

B. The need for an exemption for the Federal Gramm-Leach-Bliley Act

The GLBA, passed in 1999, broadly defines financial institutions and requires these institutions to describe how they share and protect the private information of their customers. The law is divided into three parts: the Financial Privacy Rule, which regulates collection/disclosure of private financial information; the Safeguards Rule, which stipulates financial institutions must implement security programs to protect such information; and the Pretexting provisions, which prohibit accessing private information under false pretenses. GLBA also requires financial institutions to give customers written privacy notices regarding a financial institution's information-sharing practices. Central to the GLBA are the same principles found in this and other model bills across the country: safeguarding privacy, disclosures regarding collected private information, and protections on access and use of that information. Since financial institutions have already been doing this for two decades, duplicating the requirements for financial institutions in a privacy bill draft adds unnecessary complications for businesses. An unambiguous exemption for those entities already complying with GLBA ensures businesses can process data for customers and know that the potential for confusion has been completely nullified

To assist your committee, we propose the following GLBA exemption, modeled after the GLBA exemption in the CCPA[7]:

> This [act] [title] [chapter] does not apply to a financial institution as defined by 15 U.S.C. Sec. 6809(3), or to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102).

C. The need for an exemption for the Federal Drivers Privacy Protection Act

The DDPA requires all states to protect the privacy of personal information contained in an individual's motor vehicle record. This information includes the driver's name, address, phone number, Social Security Number, driver identification number, photograph, height,

[7] The GLBA exemption in the CCPA reads as follows: "This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section 1798.150 [concerning security breach notification]." Cal. Civ. Code § 1785.145(e).

weight, gender, age, certain medical or disability information, and in some states, fingerprints. It does not include information concerning a driver's traffic violations, license status or accidents. There are important exemptions that are intended to protect the general public, including obtaining and using information for motor vehicle recalls, insurance purposes, and driver history information for background checks.

To assist your committee, we propose the following GLBA exemption, lifted from the DPPA exemption in the CCPA[8]:

> (f) This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the Driver's Privacy Protection Act of 1994 (18 U.S.C. Sec. 2721 et seq.).

2. Any state privacy law should exempt public records

There is a long-valued tradition in the United States of making public records available to the general public. The benefits of public record access and use are well-established to, among other things, combat fraud in both the public and private sectors and to more easily complete consumer transactions to meet consumer expectations.

To assist your committee, we propose the following public record exemption:

This [act] [title] [chapter] does not apply to publicly available information. For purposes of this section, publicly available information means information that is lawfully made available from federal, State, or local government records, or generally accessible or widely-distributed media.

A. Preventing and solving criminal activity

Then-FBI Director Louis Freeh testified before Congress in 1999 and noted that in 1998, his agency made more than 53,000 inquiries to commercial on-line databases "to obtain public source information regarding individuals, businesses, and organizations that are subjects of investigations." This information, according to Director Freeh, "assisted in the arrests of 393 fugitives, the identification of more than $37 million in seizable assets, the locating of 1,966 individuals wanted by law enforcement, and the locating of 3,209 witnesses wanted for questioning."[9]

---

[8] Cal. Civ. Code § 1785.145(f).

[9] *Hearing before the Senate Comm. on Appropriations Subcomm. for the Departments of Commerce, Justice, and State, and the Judiciary and Related Agencies, March 24, 1999 (Statement of Louis J. Freeh, Director of the Federal Bureau of Investigation).*

The "[Texas] Attorney General's Office routinely uses national databases provided by private resellers to track down individuals who are delinquent in their child-support payments, as well as to help locate suspects in the course of conducting consumer protection and criminal investigations. Plaintiffs' theory of liability would not just drive these resellers out of business—it would eliminate a valuable tool of law enforcement."[10]

Law enforcement agencies routinely see the benefit of information provided by commercial sources. This is true in big cities, small towns, and in between. Police in Hutchinson, Kansas (pop. 41,000) have harnessed the power of a commercial service. This program pulls together diffuse data points to serve law enforcement agencies. Police Chief Dick "'Heitschmidt said the system narrowed down an area where a suspect in a string of burglaries lived. At first, Heitschmidt said officers didn't believe the software could determine an area with any accuracy, until they later found the suspect living in the same area.'" The Hutchinson News said that the reports from commercial services using privately held and public records will "change the way police patrol [the city]", "saves the department time[,] and could possibly even save lives."[11]

B. Locating and collecting delinquent child support

The Association for Children for Enforcement of Support reports that public record information provided through commercial vendors helped locate over 75 percent of the "deadbeat parents" they sought.[12]

C. Preventing public benefit fraud; saving taxpayer money

Starting in 2011, a national consumer reporting agency partnered with the Maryland Department of Human Resources to cut down on public benefits fraud. Because of this partnership, there was a 200% reduction on the Department's payment error rate for its Supplemental Nutrition Assistance Program (SNAP).[13]

---

[10] May 8, 2009 *Brief of the State of Texas as Amicus Curiae in Support of Defendants*, *Taylor v. Acxiom Corp.*, U.S. Court of Appeals (5th Cir.) Case No. 08-41083, 41180, 41232, pp. 2-3.

[11] Stavola, Michael, *Police in Hutchinson, Kan., See Results Thanks to New Software; From locating suspects to potential accident sites, data analytics tools from are giving authorities a leg up*, The Hutchinson News, March 8, 2018, http://www.govtech.com/public-safety/Police-in-Hutchinson-Kan-See-Results-Thanks-to-New-Software.html.

[12] *Information Privacy Act, Hearings before the Comm. on Banking and Financial Services, House of Representatives, 105th Cong., 2nd Sess. (July, 28, 1998) (statement of Robert Glass).*

[13] Rebecca Lessner, *Credit rating firm helps state validate welfare recipients*, Maryland Reporter, June 25, 2015, http://marylandreporter.com/2015/06/30/credit-rating-firm-helps-state-validate-welfare-recipients/.

In 2015, a CDIA member used public record databases and identity analytics technology to help three counties in Indiana – Allen, Delaware, and Vanderburgh – find more than $4.6 million in new revenue by using a Homestead Exemption Fraud Detection system operated by LexisNexis Risk Solutions and Tax Management Associates.[14] LexisNexis has been working with Delaware County, Indiana, since 2012 and in that year, LexisNexis helped recover $1.5 million in erroneous homestead exemption claims for that county. To perform this fraud prevention, LexisNexis "went through the county database, comparing the records to information found about the property owners using LexisNexis' analytic and research technology. TMA notated property owners that had a homestead exemption filed in Indiana or anywhere else in the U.S., had a home in a trust or similar red flags."[15]

In 2004, the GAO issued a report concerning the use of "data mining" in the federal government[16]. Data mining is a pejorative term, and the GAO noted that it is also referred to as "factual data analysis," "predictive analytics," and other terms.[17] Regardless of what it is called, information collection and analysis is used because it "enables corporations and government agencies to analyze massive volumes of data quickly and relatively inexpensively."[18]

Most of the information gathering and analysis by the federal government mentioned in the GAO report contains personal information.[19] The report noted that 128 federal agencies use data mining for "improving service or performance; detecting fraud, waste and abuse; analyzing scientific and research information; managing human resources; and analyzing intelligence and detecting terrorist activities."[20] The biggest user of information compilation and analysis for the detection of fraud, waste, and abuse is the Department of Education. Not surprisingly, one of the largest users of information compilations for criminal pattern detection is the Departments of Justice.

---

[14] *LexisNexis and Tax Management Associates Identify Erroneous Tax Filings and Discover More Than $4.6 Million in New Revenue for Three Indiana Counties*, Reuters, Sept. 14, 2015, http://mobile.reuters.com/article/idUSnBw145792a+100+BSW20150914.

[15] *County Uses Fraud Solution to Unearth $1.5 Million: Relying on information provided by a fraud detection program, Indiana's Delaware County is billing property owners for unpaid taxes*, Government Technology, March 8, 2012, http://www.govtech.com/budget-finance/County-Uses-Fraud-Solution-to-Unearth-15-Million.html.

[16] *General Accounting Office, Data Mining: Federal Efforts Cover a Wide Range of Uses, GAO-04-548 (May 2004).*

[17] *Id*., at 4.

[18] *Id*., at 3.

[19] *Id*., at 3.

[20] *Id.,* at 2-3.

3. Any state privacy law should fraud prevention

Fraud in the public and private sectors may be hard to quantify but cannot be understated. Preventing fraud in for governments and businesses is an ongoing struggle. It is imperative that the private sector have robust access to a wide array of information to help businesses and governments alike prevent fraud. Many of the same points raised above on the importance of public record access apply to fraud prevention. Fraud prevention makes use of public record information, but also includes private sector records, all to help keep fraud as low as possible.

To assist your committee, we propose the following fraud prevention exemption:

> (1) This law does not apply to an activity involving the collection, authentication, maintenance, disclosure, sale, processing, communication, or use of personal information to:
>
> (a) Protect against, prevent, detect, investigate, report on, prosecute, or remediate actual or potential:
>
> (i) Fraud;
>
> (ii) Unauthorized transactions or claims;
>
> (iii) Security incidents;
>
> (iv) Malicious, deceptive, or illegal activity; or
>
> (v) Other liability;
>
> (b) Assist another person, entity, or government agency in conducting any of the activities specified in subsection (a); or
>
> (c) Comply with or defend claims under federal, state, or local laws, regulations, rules, guidance, or recommendations:
>
> (i) Setting requirements, standards, or expectations to limit or prevent corruption, money laundering, export controls;[21] or
>
> (ii) Related to any of the activities specified in subsection (a).

4. Any state privacy law should focus only on consumer information, not commercial information

If there is to be a state privacy bill, it should be focused on personal, consumer information, and should not, expressly or tacitly include commercial information (such as information about an individual acting on behalf of a business, business or commercial credit information, or employee information collected by an employer for employment related purposes). Such an approach protects consumers; meets consumer expectations; and allows

[21] *Eg.*, Int'l. Trade Administration's Export Control Regulations, or Rule 2090 of the Financial Industry Regulatory Authority (FINRA), concerning "Know Your Customer".

Texas businesses, especially small businesses, to fulfill statutory obligations as employers and compete for financing to help their businesses grow and thrive.

5. The model or approach to consider when drafting a bill

Your committee will have a lot of sources to pick and choose from once it starts drafting. There may be attractive elements of the CCPA or the WPA. Another approach your committee may wish to consider is an alternative draft being considered by the Uniform Law Commission ("ULC"). The ULC has committee, the Collection and Use of Personally Identifiable Data Act Committee, that is working to develop a model state privacy bill. This draft

> safeguards consumer trust by requiring those who do business with consumers to observe widely accepted principles of fair information and privacy practices (FIPPs), to limit their use and disclosure of consumers' data to purposes that are compatible with the original purposes for which the data was collected and for which consumers have either expressly or impliedly consented. The Act also sets clear rules for how consent must be obtained for non-compatible uses and prohibits uses that exceed the boundaries of consumer consent.

6. Conclusion

CDIA members play a critical role in American commerce. Through data and analytics, CDIA members empower economic opportunity all over the world, helping ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs. CDIA members are heavily regulated by an array of federal and state laws, including privacy laws.

As your committee discusses possible privacy legislation in 2021, we hope that you will keep in mind several core CDIA principles, that any state privacy law should (1) Exempt key existing federal privacy laws; (2) Exempt public records; (3)Allow data use for fraud prevention; and (4) Focus only on consumer information, and not commercial information.

Respectfully submitted,

Eric J. Ellman
Senior Vice President, Public Policy & Legal Affairs