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

P 202 371 0910

Writer's direct dial: +1 (202) 408-7407

CDIAONLINE.ORG

November 9, 2018

The Honorable David J. Redl
Assistant Secretary for Communications and Information
National Telecommunications and Information Administration
United States Department of Commerce
1401 Constitution Avenue, NW
Washington, DC 20230

Re: Docket No. 180821780-8780-01

Via email: privacyrfc2018@ntia.doc.gov

Dear Assistant Secretary Redl:

The Consumer Data Industry Association ("CDIA") applauds the work the NTIA has been conducting on a privacy policy, especially your willingness to meet with a broad set of stakeholders. This comment is in response to the NTIA Request for Comments on Developing the Administration's Approach to Consumer Privacy, Sept. 25, 2018. We are pleased to share our perspectives on protecting consumers' privacy and promoting an information economy that is competitive, fair, innovative and focused on consumer needs.

This comment outlines how CDIA members play a critical role in our nation's economy in ways that supports consumers, help businesses, assist non-profits, and support law enforcement and government agencies. This comment articulates our support for a federal privacy law that (1) Targets unregulated sectors in need of regulation; (2) Creates an absolute, uniform standard for the nation; (3) Exempts flows of data for fraud prevention purposes; (4) Exempts publicly available data; and (5) Does not affect, modify, limit, or supersede the operation of current federal privacy laws.

1. **CDIA members provide critical consumer-forward services to businesses, government agencies, law enforcement, and non-profits**

CDA members empower economic opportunity for consumers by helping people obtain homes, cars, student loans, jobs, volunteer opportunities, and apartments. CDIA members help reduce fraud in the public and private sectors. CDIA members work with law enforcement to locate victims, witnesses, and fugitives. CDIA members harness the

power of data in a tightly-regulated environment to provide a wide array of economic and socially beneficial services to financial institutions, businesses, governments, law enforcement, non-profits, charities, and religious organizations.

2. Consumers are protected by an array of robust federal and state laws which tightly regulate CDIA members and data flow to and from these members

CDIA members are governed by an array of federal and state laws and rules. There is a long tradition in this country of sectoral privacy regulation and that tradition should be honored if and when additional privacy laws or rules are considered. Sectoral regulation is done via laws and rules for financial privacy, like the federal Fair Credit Reporting Act ("FCRA") and the Gramm-Leach-Bliley Act ("GLBA"); health privacy, like the Health Insurance Portability and Accountability Act ("HIPAA"); children's privacy, like the Children's Online Privacy Protection Act COPPA; and driver's license information like Drivers' Privacy Protection Act ("DPPA"). A one-size-fits-all privacy law will not work. What will work, and what CDIA supports, is a national, privacy and security law to regulate sectors that are in need of additional regulation, which preserves the operation of federal laws such as the laws discussed here, and which creates an absolute, uniform federal standard. An overview of the laws and standards that regulate, supervise, or enforce against CDIA members on privacy or data security is attached as an appendix to this comment.

Fraud is a part of nearly every category of transactions in American commerce. CDIA members serve as both a bulwark against fraud and an engine to empower opportunity. Employers, landlords and volunteer organizations want to make sure they are dealing with the right person when evaluating an application for work[1], an

[1] ADP performs background checks on prospective employees. In 2007 it found that 45% of employment, education and/or credential reference checks revealed a difference of information between what the applicant provided and the source reported, http://www.screeningandselection.adp.com/pdf/screeningIndex2008.pdf. Also, a report by the Center for Identity Management and Information Protection found that a business was the point of compromise for identity theft in 50% of the cases studied, and 34% resulted directly from insider theft. A range of business types are targeted: the study found that 42% of insider theft occurs in retail businesses, and over 23% impacts private companies and insurance companies.

apartment[2], or to work with vulnerable populations.[3] People looking to perpetuate financial or violent crimes in the workplace, or seeking to avoid detection from prior bad acts, may attempt to provide fraudulent SSNs to further future or hide past criminal activity. Fraud against the government is widespread and SSN verification can help keep fraud numbers to a more manageable level.[4] Any new privacy law should not seek to prohibit or restrict consumer data when used to detect and deter potential or actual fraud.

3. Consumer data is a powerful tool to prevent fraud, enhance financial inclusion, and promote safe and sound financial decisions

Consumer data empowers risk management in multiple ways across the economy. CDIA members help rental communities screen potential tenants. Background check companies screen applicants who are applying to drive trucks across the country. Our members help lenders and others ensure that their products are right for individual customers.

If a consumer has responsibly used credit in the past, lenders and others are more likely to offer the most favorable terms – terms that previously were reserved for the wealthy, or those in a religious or ethnic majority. Similarly, a background check company may discover a past conviction of a job applicant seeking to work at a daycare center. CDIA members use data from public records and private data furnishers to give lenders, creditors, employers, landlords and others information necessary to make the best decision for the company and the consumer.

---

[2] The GAO looked at the Department of Housing and Urban Development's (HUD) Public Housing and Tenant-based Section 8 programs and found that that it "…could use enhanced data sharing to make more timely and accurate eligibility determinations." The September 2000 report noted that "HUD estimates that the lack of adequate information on applicants' and tenants' income contributed to $935 million of excess rental subsidies in 1998." *General Accounting Office, Benefit and Loan Programs: Improved Data Sharing Could Enhance Program Integrity, GAO-HEHS-00-119 (Sept. 13, 2000), 6.*

[4] Applicants for Temporary Assistance for Needy Families (TANF), a program designed to help low-income families, are required to provide their SSNs. Some agencies share SSN information to verify eligibility and identity. Between January and September 1999, New York State estimated that SSN verification saved about $72 million. *General Accounting Office, Social Security Numbers, Government Benefits from SSN Use but Could Provide Better Safeguards, GAO-02-352 (May 2002), 15, citing General Accounting Office, Benefit and Loan Programs: Improved Data Sharing Could Enhance Program Integrity, GAO-HEHS-00-119 (Sept. 13, 2000).*

Consumer data serve as an important check on human bias and assumptions, providing lenders with facts that contribute to equitable treatment for consumers. CDIA members establish an accountable and colorblind system designed both for the best interests of consumers and safety and soundness of lending institutions and other users of reports. Without this system, subjective judgements based on factors other than facts are more likely.

Consumer reports and consumer reporting agencies are regulated by the FCRA. The FCRA provides common protections for consumers, primarily the right to know what is in a report, and dispute information that has resulted in an "adverse action" to the consumer. This transparency is critical to the functioning of the consumer reporting marketplace.

Consumer reports are critical to increasing financial inclusion, for risk management, to assess whether consumers have the ability to repay their debts, to ensure safe and sound lending decisions and to make sure lenders are making their products in a fair and equitable way.

Companies, including financial institutions, retailers, landlords, government agencies and others across the economy work with CDIA members to prevent fraud. Our members' products are critical in helping companies fight back against increasingly sophisticated efforts to steal identities, money and illegally access benefits.

CDIA members help manage risk in multiple ways. By accessing publicly available data and supplementing it with additional data sources and analytics, companies are able to draw links that may not otherwise present themselves, allowing companies and government agencies to ensure that the right people are receiving the services for which they applied.

CDIA members are constantly innovating to help improve their fraud prevention and risk management tools. There is no one silver bullet to preventing identity theft, but our members are on the cutting edge of technological advances to keep fraud rates as low as possible.

4. The FCRA and GLBA are but two strong, national privacy law to protect consumers and regulate CDIA members

CDIA supports a federal privacy law that, among other things, targets unregulated sectors in need of regulation and does not affect, modify, limit, or supersede the operation of current federal privacy laws. Two of these laws are the FCRA and the GLBA.

Unlike some industry segments economy that are unregulated, companies regulated by the FCRA and GLBA exist in a highly and effectively regulated market. The FCRA has standards around how information is collected, used and disposed of. Consumers have specifically enumerated rights. Then-FTC Chairman Tim Muris 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.[5] The GLBA provides an important set of privacy standards regarding the sharing of a consumer's nonpublic personal identifying information with corporate affiliates and third parties. The GLBA allows consumers to control the sharing of information about them in many situations.

5. A federal privacy law should include broad exemptions for publicly available information

Public record access serves the public interest. Mortgages, for example, are recorded with local authorities to ensure that a property cannot be sold while it is financially encumbered. Access to public records helps to prevent public and private fraud; locates victims, witnesses and fugitives; helps to protect health and safety through criminal background checks; and more. Publicly available information and public record information are significant reasons for the success of the consumer reporting system. Since there is a strong public and constitutional interest in public records and in publicly available information, a national, preemptive privacy law should exempt from application the acquisition, storage and use of public records.

[5] FTC Chairman Tim Muris, October 4, 2001 before the Privacy 2001 conference in Cleveland.

For example, 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.[6] For law enforcement purposes, 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."[7]

6. A federal privacy law must exempt flows of data for fraud prevention

As long as there is fraud, there will be fraud prevention measures. In order to keep fraud as low as possible, a national, preemptive, contextual privacy law must exempt fraud prevention efforts. As one example of the need for CRA data for fraud prevention, "[the Texas Attorney General's Office] need[s] the private sector to help protect consumers and help combat identity fraud. Moreover, we also need the private sector to assist law enforcement." [8]

A July 2014 blog posting by the Pew Charitable Trusts highlighted how a CDIA member's "identity proofing" had saved New Jersey millions of dollars in improper unemployment insurance claims. According to Pew, applicants for unemployment compensation are asked a number of questions, like the kind of car they have and who lives at their address. "The information is then verified using the billions of public records that LexisNexis collects. The process aims to weed out potential fraudsters who might otherwise be able to collect unemployment simply by using someone's name and

[6] *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).
[7] *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).
[8] Amicus Argument of James Ho for State of Texas, *Taylor v. Acxiom Corp.*, U.S. Court of Appeals (5th Cir.) Case Nos. 08-41083, 41180, 41232, (Nov. 4, 2009).

Social Security number." For New Jersey, "[t]he payoff...has been significant. Almost a year-and-a-half into the effort, $4.4 million in payments have been stopped, and almost 650 instances of potential identity theft have been avoided."[9]

One last example of fraud prevention power is found in a public-private partnership in Maryland between the state and another CDIA member. "Starting in 2011, Equifax partnered with the Maryland Department of Human Resources to cut down on public benefits fraud. As a result of that partnership, there was a 200% reduction on the Department's payment error rate for its Supplemental Nutrition Assistance Program (SNAP)."[10]

7. Data flows are national and a federal privacy policy must be national

The California Consumer Privacy Act ("CCPA") threatens to impede national and international commerce for American businesses. Data and technology know no borders, but a California-specific system of privacy and data controls, which may be different from and conflict with whatever state comes next, and the next one after that, stifles innovation and consumer expectations. A national privacy standard requires a preemption of state privacy and data security laws. A national privacy standard must make allowances for and exempt from application the strong sectorial privacy laws that already exist, like the FCRA and the GLBA for financial privacy. We hope NTIA, in its work to create a national privacy standard, will support state preemption and exempt existing sectorial privacy laws.

---

[9] Jake Grovum, The Pew Charitable Trusts, *How 'Identity Proofing' Saved New Jersey Millions,* http://www.pewtrusts.org/en/research-and-analysis/blogs/stateline/2014/07/29/how-identity-proofing-saved-new-jersey-millions, July 29, 2014.

[10] 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/.

8. Conclusion

We appreciate this opportunity to share our views on this important issue. The companies and individual employees in our industry are committed to the highest standards of security and privacy protection and we look forward to working with you, the Administration and Congress to advance these goals. We look forward to discussing these important issues with you and your colleagues in person in the near future.

Sincerely,

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

An overview of the laws and standards that regulate, supervise, or enforce against CDIA members for privacy or data security

A number of consumer reporting agencies, are subject to the GLBA's information security requirements, and its implementing regulation, the Standards for Safeguarding Customer Information ("Safeguards Rule") promulgated by the FTC. The Safeguards Rule imposes specific standards designed to:

- Ensure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of such records; and
- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any consumer.

The Safeguards Rule requires financial institutions, as broadly defined by law, to "develop, implement, and maintain a comprehensive information security program" that includes appropriate administrative, technical and physical safeguards to achieve these objectives. This program is required to be tailored to the institution's size and complexity, the nature and scope of its activities and the sensitivity of customer information.

These and the many other provisions of the Safeguards Rule are general parameters designed to keep pace with evolving threats. Regulators anticipated that private institutions and their direct regulators and supervisors would fine-tune industry best practices over time.

CRAs are also subject to the FTC's jurisdiction over cybersecurity matters under Section 5 of the FTC Act. Under this law the FTC is empowered to take action against any business that engages in "unfair or deceptive acts or practices" ("UDAP"), which the agency has interpreted to include inadequate data security practices.

The FTC requires companies to employ safeguards for information that are "reasonable in light of the sensitivity and volume of consumer information it holds, the size and complexity of its data operations, and the cost of available tools to improve security and reduce vulnerabilities." While specific cybersecurity requirements under Section 5 are not codified, the FTC has issued detailed guidance that explains what it considers to be reasonable cybersecurity safeguards. These include practices such as encryption, use of firewalls, use of breach detection systems, maintaining physical security of objects that contain sensitive information and training employees to protect such information.

In addition to issuing detailed guidance, the FTC zealously enforces these standards, having brought over 60 cases since 2002 against businesses for putting consumer data at "unreasonable risk." It is our understanding from publicly-reported information, for example, that the FTC is the lead agency investigating the Equifax data breach.

By law, consumers have the right to dispute information in their file, and the consumer reporting agency is obligated to conduct a reasonable investigation of the dispute. Consumer reporting agencies must also independently employ reasonable procedures to assure maximum possible accuracy of the information in consumer files.

The FCRA also requires that consumer reporting companies only provide reports to legitimate companies or people with a "permissible purpose" to receive such reports, such as credit or insurance underwriting, background checks, and more. Companies' procedures must require that prospective users of credit reports identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose. The FTC has brought multiple actions over the years seeking to enforce these provision.

The federal FCRA has been around for nearly 50 years, with regular fine-tuning. Two significant revisions occurred in 1996 and 2003. In 2012, the Bureau of Consumer Financial Protection ("BCFP" or "the Bureau") began supervision and examination of the credit reporting companies for compliance with the FCRA, under authority granted to the Bureau by the Dodd Frank Wall Street Reform and Consumer Protection Act. The Bureau has examination authority over the credit reporting agencies, users of credit reports and companies that furnish information into the credit reporting agencies for incorporation into credit reports.

Since BCFP supervision began, the nationwide CRAs have been subject to essentially continuous examination cycles, where they have been examined for the adequacy of their compliance management systems, their dispute handling procedures, their procedures to ensure the maximum possible accuracy of credit reports, their credentialing procedures and other important and highly regulated functions. In this supervisory role, the BCFP examines the policies, procedures, controls and practices of credit reporting agencies. If the examiners discover any areas in which a credit reporting agency is not living up to its obligations, the BCFP can resolve the issue through the supervisory process, or, if the issue is sufficiently serious, choose to bring enforcement actions. In its "Supervisory Highlights" March 2017 Special Edition, the Bureau cited the success of this regime, concluding that it had produced a "proactive approach to compliance management" that "will reap benefits for consumers – and the lenders that use consumer reports – for many years to come."

In addition to these federal regulatory frameworks, consumer reporting agencies have numerous data security obligations under state laws. First, consumer reporting agencies may be subject to data security enforcement of state "mini-FTC Acts" that prohibit unfair or deceptive acts or practices. Further, many states require businesses that own, license or maintain personal information to implement and maintain reasonable security procedures and practices and to protect personal information from unauthorized access, destruction, use, modification or disclosure. Federal law and many states require businesses to dispose of sensitive personal information securely.

Even beyond these direct governmental requirements, additional legal requirements resulting from doing business with other major financial institutions require CRAs to secure data. The information security programs at many credit bureau financial institution customers are supervised by federal prudential regulators, i.e., the Federal Reserve, the Office of the Comptroller of the Currency, the Federal Deposit Insurance Corporation and/or the National Credit Union Administration. Under comprehensive and detailed information security standards published by the Federal Financial Institutions Examination Council, these financial institutions must oversee the information security programs of their third-party service providers, often including onsite inspections or examinations.