CONSUMER DATA INDUSTRY ASSOCIATION
Empowering Economic Opportunity
Writer's Direct Dial: 202-408-7407
Writer's Email: eellman@cdiaonline.org

February 18, 2011

Hon. Donald S. Clark
Federal Trade Commission
Office of the Secretary
600 Pennsylvania Avenue, NW
Washington, DC 20580

Via Electronic Filing

Re: Preliminary FTC Staff Report on "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers"

Dear Secretary Clark:

On behalf of the Consumer Data Industry Association (CDIA), I am pleased to file this comment on the Federal Trade Commission's ("FTC" or "Commission") above referenced preliminary staff report.[1]

By way of background, CDIA was founded in 1906 and is the international trade association that represents some 200 consumer data companies. CDIA members represent the nation's leading institutions in credit reporting, mortgage reporting, check verification, fraud prevention, risk management, employment reporting, tenant screening and collection services.

CDIA members use information in many ways that benefit commerce, consumers, law enforcement, and government. We agree with Chairman Leibowitz's assessment that "[t]echnological and business ingenuity have spawned a whole new online culture and vocabulary … that consumers have come to expect and enjoy."[2] Consumers expect and demand fast and reliable commercial transactions. These demands can often only be met by the robust consumer information products and services of our members. Consumers also expect and demand that they, their families, their friends and their neighbors engage in financial and social settings in ways that reduce fraud and keep them physically safe. CDIA members offer substantial assistance to public and private entities in achieving these benefits that many consumers never see but are undoubtedly glad they exist.

CDIA members are good stewards of largely third-party information and we hope our comments will assist the Commission in its work. To that end, we make several points: First, the collection and use of third-party data is critical to the functioning of commerce and society; second, privacy regimes should be

[1] FTC, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers*, Preliminary FTC Staff Report (Dec. 1, 2010) ("Report").
[2] Press Release, FTC Staff Issues Privacy Report Offers Framework for Consumers, Businesses, and Policymakers (Dec. 1, 2010), available at http://www.ftc.gov/opa/2010/12/privacyreport.shtm.

sectorial and voluntary; third, since data is contextual, notice, access, and choice must be viewed in relation to why it is used and who is using it; and fourth, data breach notification should be national and not subject to state regulation.

1. The collection and use of third-party data is critical to commercial and societal functions

CDIA members use third-party information in many ways, not just to promote commerce, but to assist consumers, law enforcement and government. Software and analytical tools are critical to how we manage risk in this country, how we ensure fair treatment of people, and most importantly, how we protect consumers from becoming victims of both violent and white-collar crimes of all types. The information CDIA members provide helps locate fugitives, collect delinquent debts, prevent fraud, assign credit and insurance risk, and more. Perhaps James G. Huse Jr., the Social Security Administration's inspector general said it best: "If we can't be sure when interacting that someone is who they purport to be, where are we?"[3]

Reductions in the flows of third-party data – including limits on first-party collection and choice – would impose a substantial strain on so many factors of the American and global economies that it would be extremely difficult for them to function. Here are but a few examples of how third-party information provided by CDIA members is used for socially beneficial purposes.

- Law enforcement. 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."[4]
- Child support enforcement. 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.[5]
- Fraud prevention. "We [the Texas Attorney General's Office] need the private sector to help protect consumers and help combat identity fraud. Moreover, we also need the private sector to assist law enforcement." [6]
- Homeland security. As stated by the Department of Homeland Security: "[W]e often get more accurate data from the commercial sector. In addition, the processes by which government agencies manage data often makes it difficult to acquire and needs [a] great deal of labor intensity into making it usable and accessible to other entities."[7]

---

[3] Robert O'Harrow Jr. and Jonathan Krim, *National ID Card Gaining Support,* Washington Post, Dec. 7, 2001, A1 (quoting James Huse, Inspector General of the Social Security Administration).

[4] 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).

[5] 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).*

[6] *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).

[7] The Privacy Office, Department of Homeland Security, Privacy and Technology Workshop, Official Transcript at 6 (Sept. 8-9, 2005) (comments of Grace Mastalli Principal Deputy Director for the Information Sharing and Collaboration Program at DHS), available at http://www/dhs.gov/xlibrary/assets/privacy/privacy_wkshop_09-2005_transcript_panel1.pdf, (last viewed Apr. 6, 2010).

- Social Security Numbers ("SSNs"). SSNs from third-party databases play a critical role in identifying and locating missing family members, owners of lost or stolen property, heirs, pension beneficiaries, organ and tissue donors, suspects, witnesses in criminal and civil matters, tax evaders, and parents and ex-spouses with delinquent child or spousal support obligations.[8]
- Analytics. Depersonalized data is used routinely to develop analytical systems that aid in effective and efficient fraud prevention, authentication, and identification. Various analytical systems facilitate lenders receiving best-in-class credit reports, having highly predictive credit scoring technologies available to them, and using income verification tools and data on assets. These tools are all for purposes of making safe and sound underwriting decisions so that consumers are treated fairly and receive products that make sense for them. The benefits of such analytics are well-established. For example, "[c]redit scoring…increases the consistency and objectivity of credit evaluation and thus may diminish the possibility that credit decisions will be influenced by personal characteristics or other factors prohibited by law, including race or ethnicity. In addition, faster decision-making also promotes increased competition because, by receiving information on a timelier basis, consumers can more easily shop for credit. Finally, credit scoring is accurate..." [9]
- Income verification. CDIA members often provide income verification tools to hospitals, other charities, and the government so that they can allocate the appropriate resources to people in need.[10] As financial institutions are under increasing pressure to assess the ability of individuals to repay obligations to avoid unnecessary risk to our financial system, CDIA members consistently deliver the tools necessary to meet these new regulatory requirements.

The benefits of third-party data are clear. The "miracle of instant credit" is as valid today as it was when it was first presented by then-FTC Chairman Tim Muris.[11] The Report alludes to the importance of this data when it discusses that fraud prevention, among other things, is too important to be subjected to consumer choice.[12] However, the Report does not fully embrace the value of third-party information beyond fraud prevention. In fact, it is possible that the Report could serve as a disincentive for third-party information collection and use. Specifically, the Report: (1) recommends that the collection and use of data by third-party providers be excluded from the Commission's listing of "commonly accepted practices;" (2) recommends that information service providers specifically be required to provide consumers with "reasonable access" to the data maintained about them; (3) promotes the notion that consumers should be able to opt-out of allowing first parties to enhance customer data with third-party

---

[8] *See generally*, *Hearing on Enhancing Social Security Number Privacy: Before the Subcomm. on Social Security of the House Ways and Means Comm. Subcom. on Social Security*, June 15, 2004 (107th Cong.) (statement of Prof. Fred H. Cate, Indiana University School of Law).

[9] *Report to the Congress on Credit Scoring and Its Effects on the Availability and Affordability of Credit*, Board of Governors of the Federal Reserve System, Aug. 2007, O-5.

[10] One example is the Department of Veterans Affairs which is required by law to verify the income "of certain nonservice-connected or noncompensable 0% service-connected veterans to confirm the accuracy of their [e]ligibility for VA health care[, c]opay status, and [e]nrollment Priority Group assignment." http://www4.va.gov/healtheligibility/iv/. (viewed Jan. 10, 2011).

[11] On October 4, 2001 before the Privacy 2001 Conference in Cleveland, FTC Chairman Tim Muris referred to the "miracle of instant credit" whereby a consumer can walk in to an auto dealer and "can borrow $10,000 or more from a complete stranger, and actually drive away in a new car in an hour or less." Muris also noted that this

> 'miracle' is only possible because of our credit reporting system. The system works because, without anybody's consent, very sensitive information about a person's credit history is given to the credit reporting agencies.

FTC Chairman Tim Muris, October 4, 2001 before the Privacy 2001 conference in Cleveland ("Muris").

[12] Report, vi, 54.

information; (4) suggests extraordinary and unworkable steps that merchants at point-of-sale should use to gain consent for third party sharing; and, (5) suggests an unworkable one-size-fits-all, real time notice for collection of online data that might be shared with third parties.

Limitations on the collection (including choice) of first-party information will have significant and negative impacts on the downstream collection and use of third-party data. Given the critical nature of third-party information, its loss would harm the American commercial system and the many social systems that are dependent on this data.

2. Privacy regimes should be sectorial and voluntary

We are grateful that the Report recognizes the existence and value of sectorial laws, like the Fair Credit Reporting Act ("FCRA"), and that the Report also acknowledges other sectorial laws.[13] The FCRA is among the first nationwide privacy laws and has been amended many times over the years to reflect the dynamic nature of technology, the credit reporting system and consumer reports in general. The same is true for other sectorial statutes, regulations, and guidelines.

Since data is contextual, privacy regulation should best be viewed vertically in the context of market segments rather than horizontally across industry sectors. Privacy controls can come in many forms: government statutes, regulations, and guidelines, and/or from industry standards. The dynamic nature of data transmission and global commerce demands privacy controls that are best left to industry standards. Commerce often works best when it has flexibility and speed to operate. Self-imposed privacy standards, rather than rigid laws, assist in providing the flexibility and speed businesses need and consumers demand.

The American credit reporting system may be the best example of the value of sectorial regulation. Through a combination of statutes, regulations, and guidelines, this country's credit reporting system offers extraordinary benefits to consumers, businesses, government, and law enforcement.[14] Self-regulatory initiatives can even be powerful enough to be adopted by Congress, praised by the relevant regulating agency, and promoted by consumer groups[15]. For example, CDIA and its members had in

---

[13] Report, 3-4.

[14] "[C]redit bureau data has made a wide range of credit products available to millions of households who would have been turned down as too risky just a generation ago." Barron, John M. & Michael Staten "The Value of Comprehensive Credit Reports: Lessons from the U.S. Experience", available at http://www.privacyalliance.org/resources/staten.pdf. In sharp contrast the benefits of the U.S. regime, consider the European experience:

> European consumers and financial actors cannot yet fully reap the benefits of an integrated. European retail credit market. Retail credit markets are fragmented along national lines. A variety of factors contribute to the situation. Amongst them, the existing obstacles to the cross-border access to and the effective use of the borrower's credit data. Credit data sharing between creditors is considered an essential element of the financial infrastructure that facilitates access to finance for consumers. The use of credit data in assessing borrowers' creditworthiness is key in order to enhance the quality of creditors' loans portfolio and thus reduce risks. It also assists creditors in complying with responsible lending obligations.

Report of the Expert Group on Credit Histories, May 2009 available at http://ec.europa.eu/internal_market/consultations/docs/2009/credit_histories/egch_report_en.pdf. .

[15] Of CDIA's initiatives, noted infra, n. 1, J. Howard Beales, III, Director of the Bureau of Consumer Protection, Federal Trade Commission, said that several provisions of the FACTA amendments to the FCRA "will codify many of the voluntary measurers initiated by the private sector and improve other recovery procedures already in place." *Hearing on Enhancing Social Security Number Privacy: Before the Subcomm. on Social Security of the House Ways and Means Comm. Subcom. on Social Security*, June 15, 2004 (105th Cong.) (statement of J. Howard Beales, III, Director of the Bureau of Consumer Protection, Federal Trade Commission).

place a number of initiatives for consumers that were eventually adopted as part of the 2003 amendments to the FCRA.[16] To be clear, CDIA does not support a legal mandate of voluntary, industry standards. However, we highlight Congressional adoption of some of our initiatives to show the power industry action can have to protect consumers and promote commerce.

The Gramm-Leach-Bliley Act is another good example of the value of sectorial regulation.[17] Taken together, both the GLBA and the FCRA stand as excellent examples of the perfect symmetry between sectorial laws. In this example, the GLBA regulates information flows between first and second parties (consumers and financial institutions) while the FCRA regulates information flows between second and third parties (financial institutions and consumer reporting agencies). The GLBA recognizes and exempts from the opt-out provisions of the FCRA data flows from financial institutions to consumer reporting agencies.

Privacy regimes must be contextual and, where they make sense, bear some rational relationship to other privacy principles. However, across the board, horizontal privacy regimes will rarely work for consumers, or business in particular or commerce in general.

3. Since data is contextual, notice, access, and choice must be viewed in relation to why it is used and who is using it

CDIA agrees with the Report's discussion of a sliding scale for consumer access to and correction of data.[18] Fair information practices cannot be applied monolithically. By definition, third-party information providers have no direct connection to consumers. The very nature of information flows can make it difficult for third-party providers to connect in any meaningful way with consumers to offer information use choices. More importantly, since so much data from and to third-party providers are used in so many ways to protect consumers, it would be impossible to imagine giving someone a choice to not have shared information that can be used to locate fugitives, witnesses, or child support debtors, or to verify, identify and thwart would-be fraud perpetrators, or threats to national security.

While there are many circumstances where third-party notice and choice is ill-advised, there are places where it is commonly accepted and helpful to consumers. The context is critical in determining when and where notice and choice is well-advised. Public records are but one such example.[19] The Report does not afford sufficient detail for a person to understand what would constitute a "commonly accepted practice" beyond the list provided in the Report. Also, the Report does not define the criteria to be applied to include other practices as consumer preferences and expectations evolve. Further, the Report's approach for identifying practices that do not require choice is too narrow. The use of third-party marketing

---

The Metro 2® Format is the universal, industry-created standard for reporting data to consumer reporting agencies. Of the Metro 2® Format, the National Consumer Law Center, Consumer Federation of America, Consumers Union, National Association of Consumer Advocates, and the U.S. Public Interest Research Group said "the failure to report electronically or use Metro 2 creates even more inaccuracies." *See* Public Comment of the National Consumer Law Center et al, to Office of the Comptroller of Currency, et al; Advanced Notice of Proposed Rulemaking: Furnisher Accuracy Guidelines and Procedures Pursuant to Section 312 of the Fair and Accurate Credit Transactions Act, at 16 (available at http://www.ftc.gov/os/comments/FACTA-furnishers/522110-00067.pdf).

[16] The Fair and Accurate Credit Transactions Act of 2003 ("FACTA"), Pub. L. 108-159, amended the FCRA. Among other things, this Act adopted as law several voluntary CDIA initiatives, including tradeline blocking (codified as 15 U.S.C. Sec. 1681c-2) and fraud alerts (codified as 15 U.S.C. Sec. 1681c-1). The initiatives are outlined in the House Financial Services Committee Report. *H.R. Comm. Print 108-47,at 224, Hearing on H.R. 2622, the Fair and Accurate Credit Transactions Act of 2003: Before the House Committee on Financial Services*, July 9, 2003 (108th Cong.) (statement of Stuart K. Pratt, President and CEO, Consumer Data Industry Assn.).

[17] 15 U.S.C. Secs. 6801 *et seq*. ("GLBA").

[18] Report, 74.

[19] *U.D. Registry, Inc. v. California*, 50 Cal.Rptr.3d 647 (Cal. App. 2 Dist. 2006) (holding consumers cannot force a reporting freeze of public record information in consumer reports).

information, for example, is a legitimate and widely accepted practice used by commercial, non-profit, and governmental organizations. Accordingly, we would encourage a structured approach or process for determining a set of "commonly accepted practices" that takes into account benefits of various activities, such as marketing, and the specific context involved. Such an approach should be flexible enough to address the ever-evolving nature of commerce and technology.

Notice and choice can be beneficial to consumers and society as a whole in specific, contextual circumstances. The FCRA is a good example of where consumers have a right to access and request corrections to consumer report information.[20] Through a combination of statutes, regulations, and guidelines, this country's credit reporting system offers extraordinary benefits to consumers, businesses, government, and law enforcement.[21]

The FCRA has in place the rights of consumers to access their credit information, often at no charge.[22] These disclosures are required to include the identities of entities that have requested that consumer's file.[23] The FCRA also requires that consumers receive a notice if an adverse action is taken based on information contained in their consumer report.[24] In the context of consumer reports used for employment purposes, a consumer must be given a copy of his or her consumer report if an adverse action is taken.[25] And, of course, the FCRA offers a mechanism for consumers to dispute information in their credit reports.[26] Yet, "[i]f consent were required, and consumers could decide -on a creditor-by-creditor basis -- whether they wanted their information reported, the system would collapse."[27]

The FCRA affords consumers the right to opt-out of having information shared for non-consumer initiated transactions and gives consumers the choice of receiving a consumer disclosure with a truncated Social Security number.[28] In the context of consumer reports and consumer reporting, access to consumer reports and the processing of consumer disputes make perfect sense. By contrast, the GLBA provides consumers with an opt-out for sharing of certain nonpublic personal information. This statute also recognizes and exempts from the opt-out provisions data flowing from financial institutions to consumer reporting agencies, and for other important uses.[29] This is an excellent example of information which is too societally important to be subject to consumer choice. To permit opt-out from this data flow could threaten the accuracy upon which our financial system relies, and could ultimately cost the vast majority of Americans the income building opportunities that are only afforded by a robust credit market. Existing laws and practices seem to be working well and do not cry out for additional legal regulation.

Third-party data collection often comes from public records and will include records of conviction, eviction, lien, judgment, and bankruptcy. Public health and safety, and the safety and soundness of the American financial system, makes notice and choice ill-advised for public record information.

Not all data should be subject to consumer choice. Data must be treated differently based on what that data is, who is using it, and for what purposes. To accomplish this objective, the privacy regimes should be sectorial and voluntary.

---

[20] 15 U.S.C. Sec. 1681 *et seq*.
[21] *Supra*, n. 14.
[22] 15 U.S.C. Sec., Sec. 1681g.
[23] Id. Sec. 1681g(a)(3)(A).
[24] Id. Secs. 1681m(a) and (b).
[25] Id. Sec. 1681b(b).
[26] Id. Sec. 1681j.
[27] Muris.
[28] Id, Sec.1681b(e), 1681g(a)(1).
[29] 15 U.S.C. Sec. 6802(e)(6)(A). Section 6802(e) enumerates a number of other specific exceptions where an opt-out is not required.

4. Data breach notification should be national and not subject to state regulation

Even though data knows no borders and moves efficiently across state lines, the American experience with data breach notification is a muddle of state laws. Data breach notification is best dealt with through a national standard. The volume and frequency of data and consumer movements from one state to another demands a national data breach standard.

We thank the FTC for recognizing the value of data and the importance it plays in American and global commerce. CDIA members play a critical role in enabling a fair, timely credit system, but our members go well beyond that. CDIA members use third-party information to assist consumers, commerce, law enforcement and government. Software and analytical tools are critical to how we gauge risk in this country, how we provide fair treatment of people, and most importantly, how we protect consumers from becoming victims of both violent and white-collar crimes of all types. It would be hard to imagine an efficient and orderly society without the data provided to and by consumer reporting agencies.

We hope the FTC will consider our four points of focus: First, the collection and use of third-party data is critical to the functioning of commerce and society; second, privacy regimes should be sectorial and voluntary; third, since data is contextual, notice, access, and choice must be viewed in relation to why it is used and who is using it; and finally, data breach notification should be national and not subject to state regulation.

Sincerely,

Eric J. Ellman
Vice President, Public Policy and Legal Affairs