



Writer's Direct Dial: 202-408-7407
Writer's Email: eellman@cdiaonline.org

January 28, 2011

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue, NW. Room 4725
Washington, DC 20230

Via Email: mailto:privacynoi2010@ntia.doc.gov

Re: "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework"

To Whom It May Concern:

Last month, the Department of Commerce ("Department") published the above referenced report and asked for comments on that report ("Report"). On behalf of the Consumer Data Industry Association (CDIA), I am pleased to file this comment.

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 are grateful to Secretary Locke for recognizing, in his introductory message to the Report, that information helps the U.S. to innovate and promote economic growth. To that end, we make several points.

First, since third-party information is critical for efficient commerce and societal function, in most cases this information should not be subject to notice or choice. Second, privacy regimes should be sectoral and voluntary. Third, the Department should recognize that privacy regimes are local and should not be subject to global interoperability, yet data security is global and conveys a need for standards. Finally, a data breach notification law should be national.

1. Third-party information is critical for efficient commerce, and certain third-party information should not be subject to notice or choice

A. Third-party information is critical for efficient commerce

CDIA members use third-party information in many ways to not just 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 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?"¹

Reductions in the flow of third-party data – including choice and consent -- would impose a substantial strain on so many factors of the American and global economy it would hard to imagine a functional economy without it. Here are but a few examples of how third-party information, including those from 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."²
- 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.³
- 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."⁴
- 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."⁵
- Social Security Numbers 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.⁶
- Analytics. Depersonalized data is used routinely to develop scoring systems that aid in effective and efficient fraud prevention, authentication, and identification. Scoring systems help ensure that lenders have the best-in-class credit reports, credit scoring technologies, income verification tools and data on assets for purposes of making safe and sound underwriting decisions so that

¹ 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).

² 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*).

³ 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*).

⁴ *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).

⁵ 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).

⁶ 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).

consumers are treated fairly and products 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, quicker 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...”⁷

- 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.⁸

B. Certain third-party information should not be subject to notice or choice

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 identify fraud perpetrators or threats to national security.

Just as there are circumstances where third-party notice and choice is ill-advised, there are also places where it is commonly accepted and helpful to consumers. Even for data that is not subject to sectoral laws, notice and choice will not always be beneficial for the economy or society as a whole. This context is critical in determining the value of notice and choice.

Notice and choice can be beneficial to consumers and society as a whole in specific, contextual circumstances. The federal Fair Credit Reporting Act (“FCRA”) is a good example of where consumers have a right to access and request correction of consumer report information.⁹ Through a combination of statutes, regulations, and guidelines, this country’s credit reporting system offers extraordinary benefits to consumers, businesses, government, and law enforcement.¹⁰

⁷ *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.

⁸ For example, the Department of Veterans Affairs 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.” Available at <http://www4.va.gov/healtheligibility/iv/>. (last visited Jan. 10, 2011).

⁹ 15 U.S.C. Sec. 1681 *et seq.*

¹⁰ Eg. “[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> (last visited Jan. 27, 2011). 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.

The FCRA has in place consumer rights to access their credit information at no charge.¹¹ These disclosures are required to include the identities of entities that have requested that consumer's file.¹² The FCRA also requires that consumers receive notice before an adverse action is taken based on information contained in their consumer report.¹³ And, of course, the FCRA offers a mechanism for consumers to dispute information they find.¹⁴

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.¹⁵ In the context of consumer reports and consumer reporting, access to consumer reports and the processing of consumer disputes of that data make perfect sense. By contrast, the Gramm-Leach-Bliley Act ("GLBA"), which provides consumers with an opt-out for sharing of certain nonpublic personal information, recognizes and exempts from the opt-out provisions data flows from financial institutions to consumer reporting agencies.¹⁶ This is an excellent example of information which is too societally important to be subject to consumer choice.

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, businesses, or commerce in general. 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 sectoral and voluntary.

2. Privacy regimes should be sectoral and voluntary

We are grateful that the Report recognizes the existence and value of sectoral laws, like the FCRA and GLBA, and that the Report acknowledges many other sectoral laws as well.¹⁷ The FCRA is among the first nationwide privacy laws and has been amended many times over the years to reflect the dynamic nature of the credit reporting system. The same is true for other sectoral 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 or 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 timeliness businesses need and consumers demand.

The American credit reporting system may be the best example of the value of sectoral 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.¹⁸ Self-regulatory initiatives can even be powerful enough to be adopted by Congress as law and praised by the

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 (last visited Jan. 27, 2011).

¹¹ 15 U.S.C. Sec. 1681g.

¹² *Id.*, Sec. 1681g(a)(3)(A).

¹³ *Id.*, Secs. 1681m(a) and (b).

¹⁴ *Id.*, Sec. 1681j.

¹⁵ *Id.*, Secs. 1681b(e), 1681g(a)(1).

¹⁶ *Id.*, Secs. 6801 *et seq.*, 6802(e)(6)(A).

¹⁷ Report, n. 160.

¹⁸ See, *infra*, n. 10.

relevant regulating agency. For example, CDIA and its members had in place a number of initiatives for consumers that were eventually adopted as part of the 2003 amendments to the FCRA.¹⁹ To be clear, CDIA does not support 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 GLBA is another good example of the value of sectoral regulation. Taken together, both the GLBA and the FCRA stand as excellent examples of the perfect symmetry between sectoral 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, business, or commerce in general.

3. Privacy regimes are local and should not be subject to global interoperability; data security is global and standards are important

The Report should recognize that data security is global, but privacy regulation is local. Countries and geographic regions of the world have different social norms, customs, and laws associated with privacy. The American experience is vastly different from that of many European countries, for example. The Department should recognize the varying social, cultural, and legal differences governing data privacy across the globe and it should avoid supporting forced interoperability standards in countries where social, cultural and legal norms are well-established.

Unlike privacy, which is viewed differently by various countries and regions, data security is global. While privacy rights may attach to the country where the data is collected or used, there should be international standards around data security. Data security knows no borders and there should be standards about how data is imported and exported. Data frequently crosses international boundaries to improve commerce and benefit consumers. These data flows, which can include cloud computing and global sourcing should be treated as security issues, not privacy issues. Data security standards must be flexible enough to accommodate existing and emerging technologies and to allow for systems and operations that are still yet undeveloped.

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

Although data knows no borders and moves efficiently and transparently 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, harm-based standard. The volume and frequency of data and consumers as they

¹⁹ The Fair and Accurate Credit Transactions Act of 2003 (“FACTA”), Pub. L. 108-159, amended the FCRA. Among other things, it 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.).

Of CDIA’s initiatives, 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 measures 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).

move from one state to another demands a national data breach standard. A breach that occurs without a reasonable likelihood that the information will be misused does not pose a security threat. The national data breach standard should first look to the likelihood of harm before a notice is required.

We thank the Department for recognizing the value of data and the importance it plays in American and global commerce. CDIA members play a critical role in ensuring a fast and efficient credit system, but our members go well beyond that. CDIA members use third-party data 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. It would be hard to imagine an efficient and orderly society without the data provided to and by consumer reporting agencies.

We hope the Department will consider our four points of focus: First, since third-party information is critical for efficient commerce and societal function, in most cases this information should not be subject to notice or choice. Second, privacy regimes should be sectoral and voluntary. Third, the Department should recognize that privacy regimes are local and should not be subject to global interoperability, yet data security is global and conveys a need for standards. Finally, a data breach notification law should be national.

Sincerely,

A handwritten signature in black ink, appearing to read 'E. J. Ellman', is written on a light-colored rectangular background.

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