June 13, 2010

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

RE: Information Privacy and Innovation in the Internet Economy
[Docket No. 100402174-0175-01]
RIN 0660-XA12

These comments are submitted on behalf of the more than 200 corporate members of the Consumer Data Industry Association (CDIA). CDIA is an international trade association representing a wide array of technology companies that build market-leading information products based on consumer data which enable businesses in the United States and around the globe to manage risk, comply with legal requirements, protect consumers and enable consumers to access a fair, safe and open free market of products and services delivered over the Internet and through bricks-and-mortar companies. CDIA estimates that its members' products are used more than 9 billion times a year in the United States alone.

CDIA and its members applaud the Department of Commerce's efforts to ensure that as it explores the nexus between privacy policy and innovation in the Internet economy it has a full and complete understanding of the Internet and its fundamental contribution to "U.S. innovation, prosperity, education, and political and cultural life."[1] We agree with the DOC's decision to make sure that "the Internet remains open for innovation."[2] Further, the DOC is correct when it states that the "proper use of personal information can play a critical, value-added role" in preserving what is best about the U.S. approach to the Internet.[3]

Risk Management – Third-party Databases and Analytical Innovations

CDIA's members own, operate, manage and develop the world's most sophisticated

[1] NTIA/ITA notice of its May 7, 2010 meeting published in the Federal Register, Vol. 75, No. 73/Friday, April 16, 2010.
[2] Ibid.
[3] NTIA/ITA/NIST notice published in the Federal Register, Vol. 75, No. 78/Friday, April 23, 2010.

third-party databases of consumer data used for risk management purposes both online and offline... They are also the leading providers of decision sciences tools which help users to evaluate data in order to manage risk. It is our members' innovative database designs and analytical tools which lower risk and ensure that citizens' expectations are met and that they continue their full participation in the Internet.

For example, consumers expect to be protected from the crime of identity theft. Our members' identity verification and management tools help Internet businesses to ensure that the persons with whom they are dealing are in fact the true consumers and not fraudsters. Out-of-wallet test questions based on credit reports, databases of names associated with previous fraudulent applications and an array of other data and analytical tools can be deployed to test an online applicant's identity on a real-time basis.

Consumers also expect to be treated fairly and given a price which reflects their hard work and care in managing their finances. Internet delivery of financial services is wholly dependent on our members' data in order to meet these expectations. U.S. credit reporting databases, which contain files on more than 200 million credit-active consumers and which are updated 3 billion times each month are studied the world over due to their sophistication, completeness and timeliness. Perhaps the most effective method for price comparison is Internet-based shopping and consumers can be confident that their data is the key to accessing low-cost credit for their small businesses, their children's college loans and for household credit of all types.

Victims of natural disasters find themselves in the unusual position of asking the government for help and they have an expectation that governmental services will be delivered quickly during their times of need. Often consumers who have moved out of the disaster area will seek such help via the Internet. The government turns to our members for identity verification tools which ensure consumers are served quickly and also that entitlement fraud is greatly reduced.

Consumers and the government expect U.S. businesses to obey the law. Laws such as the U.S.A. Patriot Act, Section 326 require financial institutions to properly verify the identity of their customers in order to prevent foreign and domestic terrorists from accessing and using our country's financial systems against it. Some may think that online applications for credit are a lower-risk method of attempting to work around identity verification. However, our members' innovative systems ensure that Internet transactions are as safe as an in-person application process. Similar systems help Internet orders for age-restricted products such as wine to not be shipped to minors. Age verification tools are critical for companies that must comply with the Children's Online Privacy Protection Act

As a result of the financial crisis Congress has imposed new, stricter statutory underwriting requirements on lenders. For example, the Credit Card Act of 2009 requires credit card issuers to restrict certain types of credit card offers to individuals under the age of 21. Credit card issuers, for example, must engage in a more probative underwriting process to ensure a consumer has "the ability to pay" the loan. Card issuers

must also ensure that certain credit card offers are not made to those under the age of 21 which requires that age verification tools be available for Internet transactions. This concept of measuring a consumer's ability to pay is also embedded in the financial services regulatory reform which states that a lender must "assure that consumers are offered and receive residential mortgage loans on terms that reasonably reflect their ability to repay the loans."[4] This reasonable assurance is a broad mandate that requires verification of income, assets as well as use of credit reports. Assessing a consumer's ability to pay assumes the existence of sophisticated, third-party databases and analytical tools which can be deployed instantly in an Internet transaction.

How U.S. Laws, Consumer Choice and Third-Party Data Infrastructure Used to Manage Risk

Congress has recognized the importance of ensuring that an infrastructure of third-party data used for risk management is preserved. Laws such as the federal Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*) regulate a range of data used for a set of permissible uses. The FCRA, which pre-dates the U.S. Privacy Act, the OECD's establishment of Fair Information Practices and Europe's Privacy Directive, is an excellent example of a law which provides consumers with rights necessary to balance against the fact that the data flows regulated under the act are generally not tied to consumer consent. See Appendix I for the FTC's summary of consumer rights under the FCRA.

Were consumers able to choose the data that went into their credit reports, such reports would be inherently at risk of being incomplete and inaccurate. Some consumer would simply choose to hide their nonpayment of debts. Clearly our country's financial crises has demonstrated definitively that full, complete and accurate data is necessary in every lending transaction if our financial institutions are to remain stable and so that securities backed by consumer loans are stable and perform as expected. In a different example, criminals, such as pedophiles who want to work in a daycare center or DUI-convicted bus drivers applying for a job driving a school bus, could, if given a right to chose whether or not an FCRA-regulated consumer reporting agency can compile their data, choose to not have their criminal records compiled and used by employers.

It is our view that the U.S. has distinguished itself in the world by recognizing that the principle of consumer choice cannot be applied monolithically and that risk-management is impaired where consumers are given choices to hide data that is necessary to prevent crimes, to predict risk and to ensure compliance with laws. For example, when enacting the Gramm-Leach-Bliley Act (GLBA), Title V, Congress made sure that the consumer's right to opt out of the transfer of nonpublic personal information to nonaffiliated third parties was limited. GLBA Title V, Section 502(e) stipulates that a range of third-parties can and must have access to data without the impairment of consumer choice including ensuring the transfer of data to existing laws which protect consumer data such as the

[4] Conference Base Text (H.R. 4173), "Restoring American Financial Stability Act of 2010", , Pg. 1786, lines 19-22

FCRA. GLBA also ensures that data can be used, for example, to prevent fraud (including identity verification), for public safety purposes, for law enforcement and to complete transactions. A full accounting of the exceptions to consumer choice can be found in Appendix II of this letter.

Laws which govern how Internet data flows involving consumer data must account for the necessity of ensuring continued innovation in the construction of risk-management systems. An inappropriate application of consumer choice to Internet data flows could choke off the innovative risk-management data systems which are created in this country only because of the careful balancing of individual protections with important societal benefits which U.S. law strikes. Third-party risk management databases are designed to comply with a plethora of legal regimes including, to name just a few, the Fair Credit Reporting Act, the Driver's Privacy Protection Act, the Health Insurance Portability and Privacy Act, the Gramm-Leach-Bliley Act, Title V, the Children's Online Privacy Protection Act, and also Section 5 of the Federal Trade Commission Act. Internet privacy laws will prevent flows of data that are critical to our

International Privacy Laws and Trans-border Data Flows

While today risk-management data is often compiled and maintained on a country-specific it is CDIA's view that the arbitrary harmonizing of legal regimes which regulate the free flow of consumer data used for risk management would be the wrong approach. As the DOC's own Federal Register notice suggests, our U.S. privacy framework is multi-faceted and "[i]n many, though not all cases, this has been a formula for success to build on."

CDIA and its members regularly participate in international dialogues regarding data flows. These include many of the ones discussed in the DOC notice such as the Safe Harbor Framework between the European Union and the United States, the Asia Pacific Economic Cooperation Privacy Framework discussions for implementation of trans-border data flows, various International Standards Organization discussions of privacy as well as World Bank-hosted Task Forces on international standards for credit reporting. Such discussions should continue and the role of the United States should be to ensure that the nature and success of U.S. laws and their operation is fully understood in these dialogues.

Conclusion

Consumer data which flows from the Internet will continue to increase as consumers shift their lives to this medium. CDIA's members will continue to serve as the vanguard when it comes to ensuring that risk management priorities are central to this mode of commerce. The DOC should make every effort to ensure that regulation of data flows does not impair in any way the construction of data bases and the ensuring innovative products which protect consumers and ensure their fair treatment.

Sincerely,

Stuart K. Pratt
President & CEO

APPENDIX I

A Summary of Your Rights Under the Fair Credit Reporting Act

The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Here is a summary of your major rights under the FCRA. **For more information, including information about additional rights, go to www.ftc.gov/credit or write to: Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.**

C **You must be told if information in your file has been used against you.** Anyone who uses a credit report or another type of consumer report to deny your application for credit, insurance, or employment – or to take another adverse action against you – must tell you, and must give you the name, address, and phone number of the agency that provided the information.

C **You have the right to know what is in your file.** You may request and obtain all the information about you in the files of a consumer reporting agency (your "file disclosure"). You will be required to provide proper identification, which may include your Social Security number. In many cases, the disclosure will be free. You are entitled to a free file disclosure if:

C a person has taken adverse action against you because of information in your credit report;

C you are the victim of identify theft and place a fraud alert in your file;

C your file contains inaccurate information as a result of fraud;

C you are on public assistance;

C you are unemployed but expect to apply for employment within 60 days.

In addition, by September 2005 all consumers will be entitled to one free disclosure every 12 months upon request from each nationwide credit bureau and from nationwide specialty consumer reporting agencies. See www.ftc.gov/credit for additional information.

C **You have the right to ask for a credit score.** Credit scores are numerical summaries of your credit-worthiness based on information from credit bureaus. You may request a credit score from consumer reporting agencies that create scores or distribute scores used in residential real property loans, but you will have to pay for it. In some mortgage transactions, you will receive credit score information for free from the mortgage lender.

C **You have the right to dispute incomplete or inaccurate information.** If you identify information in your file that is incomplete or inaccurate, and report it to the consumer reporting agency, the agency must investigate unless your dispute is frivolous. See www.ftc.gov/credit for an explanation of dispute procedures.

C **Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.** Inaccurate, incomplete or unverifiable information must be removed or corrected, usually within 30 days. However, a consumer reporting agency may continue to report information it has verified as accurate.

C **Consumer reporting agencies may not report outdated negative information.** In most cases, a consumer reporting agency may not report negative information that is more than seven years old, or bankruptcies that are more than 10 years old.

C **Access to your file is limited.** A consumer reporting agency may provide information about you only to people with a valid need -- usually to consider an application with a creditor, insurer, employer, landlord, or other business. The FCRA specifies those with a valid need for access.

C **You must give your consent for reports to be provided to employers.** A consumer reporting agency may not give out information about you to your employer, or a potential employer, without your written consent given to the employer. Written consent generally is not required in the trucking industry. For more information, go to www.ftc.gov/credit.

C **You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.** Unsolicited "prescreened" offers for credit and insurance must include a toll-free phone number you can call if you choose to remove your name and address from the

lists these offers are based on. You may opt-out with the nationwide credit bureaus at 1-888-5-OPTOUT (1-888-567-8688).

C **You may seek damages from violators.** If a consumer reporting agency, or, in some cases, a user of consumer reports or a furnisher of information to a consumer reporting agency violates the FCRA, you may be able to sue in state or federal court.

C **Identity theft victims and active duty military personnel have additional rights.** For more information, visit www.ftc.gov/credit.

States may enforce the FCRA, and many states have their own consumer reporting laws. In some cases, you may have more rights under state law. For more information, contact your state or local consumer protection agency or your state Attorney General.

APPENDIX II

(e) GENERAL EXCEPTIONS.—Subsections (a) and (b)
14 shall not prohibit the disclosure of nonpublic personal
15 information—
16 (1) as necessary to effect, administer, or en17
force a transaction requested or authorized by the
18 consumer, or in connection with—
19 (A) servicing or processing a financial
20 product or service requested or authorized by
21 the consumer;
22 (B) maintaining or servicing the con23
sumer's account with the financial institution,
24 or with another entity as part of a private label
1 credit card program or other extension of credit
2 on behalf of such entity; or
3 (C) a proposed or actual securitization,
4 secondary market sale (including sales of serv5
icing rights), or similar transaction related to a
6 transaction of the consumer;
7 (2) with the consent or at the direction of the
8 consumer;
9 (3)(A) to protect the confidentiality or security
10 of the financial institution's records pertaining to
11 the consumer, the service or product, or the trans12
action therein; (B) to protect against or prevent ac13
tual or potential fraud, unauthorized transactions,
14 claims, or other liability; (C) for required institu15
tional risk control, or for resolving customer disputes
16 or inquiries; (D) to persons holding a legal or bene17
ficial interest relating to the consumer; or (E) to
18 persons acting in a fiduciary or representative capac19
ity on behalf of the consumer;
20 (4) to provide information to insurance rate ad21
visory organizations, guaranty funds or agencies, ap22
plicable rating agencies of the financial institution,
23 persons assessing the institution's compliance with
24 industry standards, and the institution's attorneys,
25 accountants, and auditors;
1 (5) to the extent specifically permitted or re2
quired under other provisions of law and in accord3
ance with the Right to Financial Privacy Act of
4 1978, to law enforcement agencies (including a Fed5
eral functional regulator, the Secretary of the Treas6
ury with respect to subchapter II of chapter 53 of
7 title 31, United States Code, and chapter 2 of title
8 I of Public Law 91–508 (12 U.S.C. 1951–1959), a
9 State insurance authority, or the Federal Trade
10 Commission), self-regulatory organizations, or for an
11 investigation on a matter related to public safety;
12 (6)(A) to a consumer reporting agency in ac13
cordance with the Fair Credit Reporting Act, or (B)
14 from a consumer report reported by a consumer re15
porting agency;
16 (7) in connection with a proposed or actual
17 sale, merger, transfer, or exchange of all or a por18

tion of a business or operating unit if the disclosure
19 of nonpublic personal information concerns solely
20 consumers of such business or unit; or
21 (8) to comply with Federal, State, or local laws,
22 rules, and other applicable legal requirements; to
23 comply with a properly authorized civil, criminal, or
24 regulatory investigation or subpoena or summons by
25 Federal, State, or local authorities; or to respond to
1 judicial process or government regulatory authorities
2 having jurisdiction over the financial institution for
3 examination, compliance, or other purposes as au
thorized by law.