STATEMENT OF STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION

WASHINGTON, D.C.

Hearing on

"Privacy: the Use of Commercial Information Resellers by Federal Agencies"

Subcommittee on Information Policy, Census and National Archives

Committee on Oversight and Government Reform

United States House of Representatives

Washington, D.C.

Tuesday, March 11, 2008

Chairman Clay, Ranking Member Turner and Members of this Subcommittee, thank you for the opportunity to appear before you here today.

My name is Stuart Pratt, and I am President and CEO of the Consumer Data Industry Association, CDIA. CDIA is the international trade association representing over 300 consumer data companies that provide fraud prevention and risk management products, credit and mortgage reports, tenant and employment screening services, check fraud and verification services, systems for insurance underwriting and also collection services.

There are 3 main points that I plan to discuss with you this afternoon:

1) The Recognized value of CDIA members' systems;
2) CDIA members are heavily regulated, and their reasonable, lawful collection, use and sale of consumer data are governed by a wide variety of laws;
3) Comments on H.R 4791.

I) THE RECOGNIZED VALUE OF CDIA MEMBERS' SYSTEMS

First, I would like to discuss how the government uses our members' products and services. We believe this is an important context for the committee as it continues to consider action on H.R. 4791.

Government's use of CDIA member products brings value to citizens individually and to the government which works on their behalf. CDIA's members are the leading companies producing consumer data products and services for both the private and public sector. Consider the following examples of uses of our members' products and services:

- Assisting lenders, insurance companies, landlords and others to make risk-based decisions with relevant data about the individual applying for the benefit;
- Preventing money laundering and terrorist financing;

- Enforcing child support orders;[1]
- Working with the IRS to locate assets of tax evaders;
- Assisting law enforcement and private agencies locate missing and exploited children through location tools;
- Researching fugitives, such as determining assets held by individuals of interest through the use of investigative tools which allow law enforcement agencies to tie together disparate data on given individuals;
- Witness location;
- Entitlement fraud prevention, eligibility determinations, and identity verification;
- Background screening for employment and security clearances; and
- Disaster assistance.

Our prior testimony before the House Judiciary Committee in 2006, attached as Supplement A, goes through in detail what government representatives themselves have said about the value they derive from the use of consumer reporting agencies and other consumer data companies.

II) CDIA MEMBERS ARE HEAVILY REGULATED

Equal in importance to knowing that our members' products bring great value by ensuring tax payers' money is well-spent, that government resources are used effectively, that government databases are made more accurate, that fraud is reduced and that laws are fairly enforced all for the benefit of citizens is the fact that many of these products are heavily regulated under current federal laws. This, too, is important context as the committee considers the merits of H.R. 4791.

[1] In 2004 there were 5.5 million location searches conducted by child support enforcement agencies to enforce court orders.

The federal government is also bound by these limitations, meaning that any data they obtain from regulated entities must be used only for specifically enumerated "permissible purposes" if the data is obtained from a consumer reporting agency, and subject to other limits if obtained from CDIA member companies regulated under Gramm-Leach-Bliley Act (GLB) or other laws.

Companies in our membership are not only subject to Section 5 of the FTC Act (unfairness and deception), and a range of state laws that regulate PII, but face significant federal regulations that govern many of their operations:

a) Fair Credit Reporting Act (FCRA)

It is important to note that not only was the Fair Credit Reporting Act enacted before the Privacy Act of 1974 (and OMB implementing guidelines therein), the OECD Guidelines of 1980 and the Gramm-Leach-Bliley Act of 1999 (and implementing regulations therein), the E-Government Act of 2002 and the Federal Information Security Management Act of 2002, but it has also been the focus of careful oversight by the Congress, resulting in significant changes in both 1996 and again in 2003. There is no other law that is so current in ensuring consumer rights and protections are adequate.

The FCRA applies to both the private and public sectors, and thus is extremely relevant to today's discussion.

The FCRA regulates any use of personal information (whether obtained from a public or private source) defined as a consumer report. A consumer report is defined as data which is gathered and shared with a third party for a determination of a consumer's eligibility for enumerated permissible purposes. This concept of an eligibility test is a key to understanding how Federal laws regulate personal information. The United States has a law which makes clear that any third-party supplied data that is used to accept or deny, for example, my application for a government entitlement, employment, credit (e.g.,

student loans), insurance, and any other transaction initiated by the consumer where there is a legitimate business need.

The breadth of the application of the FCRA to how data is used to include or exclude a consumer is enormous. If a decision maker, including a government agency, uses a consumer report as a basis for denying a consumer a particular benefit, the consumer has the right to be notified when a consumer report has been used to take an adverse action, and he/she can obtain a free copy of his/her consumer report that was the basis of the decision.

The FCRA provides significant rights to consumers:

- The right of access:

Consumers have an absolute right at any time to obtain the disclosure of all information in their file at the time of the request. This right is enhanced by requirements that mandate free disclosure under a variety of circumstances, including where there is suspected fraud, where a consumer is unemployed and seeking employment, or where a consumer is receiving public assistance and thus may not have the means to pay. Further, for some specific companies – credit bureaus – consumers have a right to obtain their consumer report annually free of charge.

This right of access not only provides consumers with the opportunity to see information about them, but also provides them with the right to know who has seen or reviewed information in the consumer's file.

- The right of correction:

Consumers may dispute any information in the file free of charge, and there is a very short time frame to respond.

- Accuracy:

All such products are regulated for accuracy with a "reasonable procedures to ensure maximum possible accuracy" standard, a standard that was first enacted in 1970, and has withstood the test of time and two major revisions of the FCRA. Further, all sources which provide data to consumer reporting agencies must also adhere to a standard of accuracy which, as a result of the FACT Act, now includes new rulemaking powers for the FTC and functional bank regulators.

- The right to only have the data used for specific, enumerated purposes:

The FCRA enumerates very specific "permissible purposes" that a user of a consumer report can do with a consumer report, such as the provision of credit or employment. These limited uses protect consumers from broad disclosure and prevent the use of this data for marketing or other purposes.

- The right to a notice of all other rights:

With every disclosure of a file, consumers receive a notice providing a complete listing of all consumer rights.

b) Financial institutions under the Gramm-Leach-Bliley Act:

Outside of the FCRA, Congress has applied different standards of protection to data that are appropriate to the use and sensitivity of data. Similar to the FCRA, GLB establishes a number of restrictions on how data can be used, along with wide ranging privacy and data security standards. CDIA members produce and sell a range of fraud prevention (e.g., identity verification to prevent entitlement fraud) and location products (e.g. locating a non-custodial parent for purposes of enforcing a child support order) which are governed by other laws such as GLB.

III) COMMENTS ON H.R. 4791

Finally, we would like to comment on H.R. 4791, which touches on many of the issues we have raised today.

a) Role of "data broker" should not be primary focus; how government uses data is the relevant question.

There is a general misperception that this legislation carries forward: that all "data brokers" are unregulated, and possess vast amounts of data which may be used to profile consumers.

Instead, we believe that the Committee and this legislation should focus on whether the government legally obtained the information that it uses, for example by demonstrating that it had a permissible purpose for obtaining the data under the FCRA, and that it intended to use the data only for those limited purposes, and whether or not it actually followed those rules. In other words, if the government uses data that it obtains in lawful ways, and protects that data from unauthorized access and use, it should not matter whether the data was obtained from a public source or a regulated entity. On the other hand, if it misrepresents how it intends to use data, then that should be investigated.

We therefore believe the data broker provisions should be struck, and the proposed law should simply focus on the legal status of the data which is being acquired and then managed.

However, absent a willingness to take this step, we urge the Committee to exclude entities subject to the GLBA privacy rules and consumer reporting agencies regulated under FCRA (and all products produced therein), along with and distributors of publicly available data from the definition of data broker.

If, as discussed above, the goal of this legislation is to determine possibly unregulated uses of private sector data, then regulated entities are, by definition not contributing to this perceived problem, and should be exempted from these requirements. These time-tested statutes already protect consumers' information before it is provided to the government, and duplicative or contradictory requirements should not be imposed.

b) Requirements of this legislation are unnecessary and possibly inconsistent with current law for CDIA members

a. Privacy Impact Assessments (PIAs) are unnecessary in this context

As OMB has recognized, for regulated entities under GLB, the concept of a PIA does not make sense. Generally the products that we are referring to are simple look up services to find a non-custodial parent for purposes of child support enforcement or a delinquent government-backed student loan held by the Department of Education, or a tenant screen for a prospective HUD tenant, and OMB Guidance has explicitly exempted these types of services from PIA requirements.[2]

b. Section 9 requirements are inconsistent with current law

Many of the requirements of this Act that would place on regulated entities are inconsistent with FCRA and GLB, and thus could make compliance difficult. For instance, the accuracy standard for consumer reporting agencies, as discussed above, is "reasonable procedures to ensure maximum accuracy." The accuracy standard that would be required under this Act is fundamentally different, and could make it more difficult for consumer reporting agencies to comply. In fact, as discussed in our prior testimony, data

[2] Guidance given by the OMB in Memorandum M-03-22, paragraph f of Section II.B of Attachment A: "Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (*Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement*)." (Emphasis added.)

provided to the federal government by CDIA members is generally *more accurate* than data the federal government collects itself or obtains from other sources.[3] Similarly, although the data security standard in the bill is similar to the GLB standard that regulated entities have to comply with, it is different enough that compliance could be complicated.

Therefore, for these additional reasons we have suggested exempting regulated entities from the coverage of this act – they already follow the standards that are equal to or more stringent than the standards that would be required by this legislation, so requiring them to comply with this additional program does not improve either data quality or consumer protections.

b) Data security/Data breach provisions

We agree that the government should secure data much as our members do today, and have advocated for the expansion of GLB Safeguards requirements beyond financial institutions. GAO reports suggest progress has been made, but also that more could be done (see "Information Security - Protecting Personally Identifiable Information - January 2008). It appears many agencies are taking more steps today and that current laws such as the Federal Information Security Management Act (FISMA), executive orders issued by OMB, and NIST technical standards establish prescriptive duties and provide helpful guidelines for implementation of data security.

Unfortunately, however, federal, state and local governments and educational institutions are the source of 60% of all data breaches. When governments and universities suffer

[3] Grace Mastalli, Principle Deputy Director for the Information Sharing and Collaboration Program for the Department of Homeland Security stated that CDIA-member products:

- are more accurate than government databases: "…commercial database providers provide accurate data – often more accurate than some that we have, because they spend the time cleaning it and verifying it and have matching capabilities that we in government have not yet invested in;"
- "in many respects, the commercial enterprises have done better jobs of organizing and, what I call 'cleaning' data to eliminate errors in data."

breaches, sensitive personally identifiable information is frequently lost, creating some risk of identity theft.

We agree the government should notify consumers where there is a breach of sensitive personal information (as opposed to just personal information). Consistent with the FTC, we believe that notification is appropriate where there is a significant risk of identity theft.

It is important to understand the role that CDIA members play after someone else has a breach. When a government entity, educational institution or private company suffers a data breach, CDIA members are usually called upon to help, even if they have absolutely no relationship with the breached entity, and often are forced to bear significant costs as a result of a breach with little or no opportunity to recoup costs. For instance, when a data breach notification is sent to consumers, the notice inevitably suggests that consumers call one of the three nation-wide credit bureaus. However, the credit bureaus are then often flooded with calls with little or no notice, and often have to scramble to ensure that their call centers are adequately staffed to deal with the increased demand. Further, consumers often expect that the credit bureau is going to know about the breach and have answers as to what happened and what their level of risk is, when the bureau may find out about the notification only through the increased call volume.

Therefore, we believe that it is appropriate to require the federal government to provide pre-notification to credit bureaus, so they can prepare for a possible increase in consumer calls, along with encouraging the federal government to offer remediation services, such as credit monitoring services, to consumers who are at increased risk of identity theft.

CDIA-member companies take identity theft and data security very seriously, and have been proactively on the cutting edge of developing a number of significant products and processes that help consumers and businesses protect themselves from identity theft, and mitigate its affects if it does occur.

For instance, CDIA member companies:

- have developed world-class tools for businesses to assist them in fraud detection and authentication efforts to help them identify fraud and ensure that the person that they are doing business with is indeed who they claim they are;
- pioneered the use of fraud alerts for consumers years before that idea was codified in the FACT Act in 2003;
- encouraged data furnishers to supply encrypted data;
- have developed credit monitoring and other services that enable consumers to proactively protect themselves from identity theft; and
- proactively established the availability for consumers to obtain a credit freeze across the country, even in states where the state legislature has not provided such an ability;

In part because of these tools, along with increased consumer education and awareness, including use of credit-file monitoring products that help consumers identify a problem while it is still easy to have it corrected, more vigorous law enforcement and more attention by the business community, including wider use of our members' fraud-prevention and identity-verification products, which help businesses stop fraud before it happens, all of the major investigations into identity-theft have found a decline in identity theft rates and in the costs to consumers and businesses across the board, as the charts in Supplement B demonstrate.

c) Other issues:

Section 3. The definition of "personally identifiable information" is extraordinarily broad, and may capture anonymous data, which by definition does not include PII.

Section 9. Subclause (d)(2)(C)(i)(II) establishes penalties for supplying inaccurate information “if the entity knows or has reason to know that the information being provided is inaccurate." However, entities sometimes intentionally provide inaccurate information, for their investigation, because the recipient wants both the accurate and the inaccurate information. This is particularly true in the case of a law enforcement

activity. Consider the case of someone with several aliases – law enforcement may want to know what other aliases are, even though they are not accurate.

CONCLUSION

In conclusion, CDIA's members create incredible value for government agencies. The consumer data industry is a significantly regulated industry through sector-specific laws which tailor the component information use principles to the types of data, risks and uses involved. Our nation remains at the forefront of enacting enforceable laws and regulations with which our members commit themselves with complying each and every day.

We appreciate this opportunity to testify and welcome your questions.