



STATEMENT OF
STUART K. PRATT
CONSUMER DATA INDUSTRY ASSOCIATION
BEFORE THE
House Energy and Commerce Committee
Subcommittee on Commerce, Manufacturing and Trade
ON
“Internet Privacy: The Impact and Burdon of EU Regulation”

Thursday, September 15, 2011

Chairman Bono-Mack, Ranking Member Butterfield, and members of the Subcommittee, my name is Stuart Pratt, and I am president and CEO of the Consumer Data Industry Association (CDIA). Thank you for this opportunity to testify.

CDIA is an international trade association with more than 190 member companies, providing our nation's businesses with the data tools necessary to manage risk in a wide range of consumer transactions. These products include credit and mortgage reports, identity verification tools, law enforcement investigative products, fraudulent check transaction identification systems, employment screening, tenant screening, depository account opening tools, decision sciences technologies, locator services and collections. Our members' data and the products and services based on it, ensure that consumers benefit from fair and safe transactions, broader competition and access to a market which is innovative and focused on their needs. We estimate that the industry's products are used in more than nine billion transactions per year.

My testimony today will focus on:

- Why it is important to preserve how consumer data is used in this country to protect consumers and enable US businesses to effectively manage risks.
- How US laws already protect consumers and successfully govern flows of data that are critical to the operation of our nation's economy.
- Why the fact that decisions about how to regulate the flow of data made by our country's trading partners and allies differ from those of the United States should

not stand as an argument for changing our country's approach to protecting consumers and enabling the most innovative data marketplace in the world.

CDIA MEMBERS' DATA AND TECHNOLOGIES HELP BOTH THE PUBLIC AND PRIVATE SECTORS TO PROTECT CONSUMERS AND MANAGE RISK

Whether it is counter terrorism efforts, locating a child who has been kidnapped, preventing a violent criminal from taking a job with access to children or the elderly or ensuring the safety and soundness of lending decisions our members' innovative data bases, software and analytical tools are critical to how we manage risk in this country, ensure fair treatment and most importantly, how we protect consumers from becoming victims of both violent and white-collar crimes of all types.

In reviewing the following examples of how our members' products, software and databases protect consumers and mitigate risk you'll see why it is critical that we do not alter our domestic marketplace for consumer data and why our marketplace is such a success today. :

- Helping public and private sector investigators to prevent money laundering and terrorist financing.
- Ensuring lenders have 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 consumers are treated fairly and products make sense for them.

- Bringing transparency to the underlying value of collateralized debt obligations and in doing so ensuring our nation's money supply is adequate which militates against the possibility and severity of future economic crises.
- Enforcing child support orders through the use of sophisticated location tools so children of single parents have the resources they need.
- Assisting law enforcement and private agencies which locate missing and exploited children through location tools.
- Researching fugitives, assets held by individuals of interest through the use of investigative tools which allow law enforcement agencies tie together disparate data on given individuals and thus to most effectively target limited manpower resources.
- Witness location through use of location tools for all types of court proceedings.
- Reducing government expense through entitlement fraud prevention, eligibility determinations, and identity verification.
- Making available both local and nationwide background screening tools to ensure, for example, that pedophiles don't gain access to daycare centers or those convicted of driving while under the influence do not drive school buses or vans for elder care centers.
- Helping a local charity hospital to find individuals who have chosen to avoid paying bills when they have the ability to do so.
- Producing sophisticated background screening tools for security clearances, including those with national security implications.
- Improving disaster assistance responses through the use of cross-matched databases that help first-responders to quickly aid those in need and prevent fraudsters from gaming these efforts for personal gain.

Not only do our members' technologies and innovation protect us and ensure that we are managing risk in this country, but they reduce costs and labor intensity. Risk management is not merely the domain of the largest government agencies or corporations in America; it is available to companies of all sizes thanks to our members' investments. Consider the following scenarios:

Scenario 1 – Effective Use of Limited Resources

The following example was given during a Department of Homeland Security meeting on use of data by the department:

“One extremely well-known law enforcement intelligence example from immediately post 9/11 was when there was a now well-publicized threat...that there might be cells of terrorists training for scuba diving underwater bombing, similar to those that trained for 9/11 to fly – but not land – planes. How does the government best acquire that? The FBI applied the standard shoe- leather approach – spent millions of dollars sending out every agent in every office in the country to identify certified scuba training schools. The alternative could and should have been for the Federal government to be able to buy that data for a couple of hundred dollars from a commercial provider, and to use that baseline and law enforcement resources, starting with the commercial baseline.”

Scenario 2 – Lowering Costs/Expanding Access to Best-in-Class Tools

One commercial database provider charges just \$25 for an instant comprehensive search of multiple criminal record sources, including fugitive files, state and county criminal record repositories, proprietary criminal record information, and prison, parole and release files, representing more than 100 million criminal records across the United States. In contrast, an in-person, local search of one local courthouse for felony and misdemeanor records takes 3 business days and costs \$16 plus courthouse fees. An in-person search of every county courthouse would cost \$48,544 (3,034 county governments times \$16). Similarly, a state sexual offender search costs just \$9 and includes states that do not provide online registries of sexual offenders. An in-person search of sexual offender records in all 50 states would cost \$800.

Scenario 3 – Preventing Identity Theft & Limiting Indebtedness

A national credit card issuer reports that they approve more than 19 million applications for credit every year. In fact they process more than 90,000 applications every day, with an approval rate of approximately sixty percent. This creditor reports that they identify one fraudulent account for every 1,613 applications approved. This means that the tools our members provided were preventing fraud in more than 99.9 percent of the transactions processed. These data also tell us that the lender is doing an effective job of approving consumers who truly qualify for credit and denying consumers who are overextended and should not increase their debt burdens.

**CURRENT LAWS REGULATING DATA FLOWS PROTECT CONSUMERS AND
ENCOURAGE INNOVATION**

The United States is on the forefront of establishing sector-specific and enforceable laws regulating uses of personal information of many types. The list of laws is extensive and includes but is not limited to the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.), The Gramm-Leach-Bliley Act (Pub. L. 106-102, Title V), the Health Insurance Portability and Accountability Act (Pub. L. 104-191), and the Drivers Privacy Protection Act (18 U.S.C. 2721 et seq.). CDIA believes this sector-by-sector approach has not just worked well, but has ensured that the United States has both marketplace that puts consumers first and one that is the most robust, innovative and effective. Following are more probative descriptions of some of these laws, the rights of consumers and also the types of products that fall within the scope of the law.

Fair Credit Reporting Act

Key to understanding the role of the FCRA is the fact that it 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 FCRA regulates an extraordinarily broad range of personal information uses. 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. Again, this law applies equally to governmental uses and not

merely to the private sector and provides us as consumers with a full complement of rights to protect and empower us. Consider the following:

- The right of access – consumers may request at any time a disclosure of all information in their file at the time of the request. This right is enhanced by requirements that the cost of such disclosure must be free under a variety of circumstances including once per year upon request, where there is suspected fraud, where a consumer is unemployed and seeking employment, when a consumer places a fraud alert on his or her file, or where a consumer is receiving public assistance and thus would not have the means to pay. Note that the right of access is absolute since the term file is defined in the FCRA and it includes the base information from which a consumer report is produced.

- The right of correction – a consumer may dispute any information in the file. The right of dispute is absolute and no fee may be charged.

- The right to know who has seen or reviewed information in the consumer’s file – as part of the right of access, a consumer must see all “inquiries” made to the file and these inquiries include the trade name of the consumer and upon request, a disclosure of contact information, if available, for any inquirer to the consumer’s file.

- The right to deny use of the file except for transactions initiated by the consumer – consumers have the right to opt out of non- initiated transactions, such as a mailed offer for a new credit card.

- The right to be notified when a consumer report has been used to take an adverse action.

This right ensures that I can act on all of the other rights enumerated above.

- Beyond the rights discussed above, with every disclosure of a file, consumers receive a notice providing a complete listing all consumer rights.

- Finally, all such products are regulated for accuracy with a “reasonable procedures to ensure maximum possible accuracy” standard. 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 federal agencies.

Gramm-Leach-Bliley Act

Not all consumer data products are used for eligibility determinations regulated by the FCRA. Congress has applied different standards of protection that are appropriate to the use and the sensitivity of the data. We refer to these tools as Reference, Verification and Information services or RVI services. RVI services are used not only to identify fraud, but also to locate and verify information for the public and private sectors.

Fraud prevention systems, for example, aren't regulated under FCRA because no decision to approve or deny is made using these data. Annually businesses conduct an average more than 2.6 billion searches to check for fraudulent transactions. As the fraud problem has grown, industry has been forced to increase the complexity and

sophistication of the fraud detection tools they use. While fraud detection tools may differ, there are four key models used.

- Fraud databases – check for possible suspicious elements of customer information.

These databases include past identities and records that have been used in known frauds, suspect phone numbers or addresses, and records of inconsistent issue dates of SSNs and the given birth years.

- Identity verification products – crosscheck for consistency in identifying information supplied by the consumer by utilizing other sources of known data about the consumer.

Identity thieves must change pieces of information in their victim's files to avoid alerting others of their presence. Inconsistencies in name, address, or SSN associated with a name raise suspicions of possible fraud.

- Quantitative fraud prediction models – calculate fraud scores that predict the likelihood an application or proposed transaction is fraudulent. The power of these models is their ability to assess the cumulative significance of small inconsistencies or problems that may appear insignificant in isolation.

- Identity element approaches – use the analysis of pooled applications and other data to detect anomalies in typical business activity to identify potential fraudulent activity.

These tools generally use anonymous consumer information to create macro-models of applications or credit card usage that deviates from normal information or spending

patterns, as well as a series of applications with a common work number or address but under different names, or even the identification and further attention to geographical areas where there are spikes in what may be fraudulent activity.

The largest users of fraud detection tools are financial businesses, accounting for approximately 78 percent of all users. However, there are many non- financial business uses for fraud detection tools. Users include:

- Governmental agencies – Fraud detection tools are used by the IRS to locate assets of tax evaders, state agencies to find individuals who owe child support, law enforcement to assist in investigations, and by various federal and state agencies for employment background checks.

- Private use – Journalists use fraud detection services to locate sources, attorneys to find witnesses, and individuals use them to do background checks on childcare providers.

CDIA's members are also the leading location services providers in the United States.

These products are also not regulated under FCRA since no decision is based on the data used. These services, which help users locate individuals, are a key business-to-business tool that creates great value for consumers and business alike. Locator services depend on a variety of matching elements. Consider the following examples of location service uses of a year's time:

- There were 5.5 million location searches conducted by child support enforcement agencies to enforce court orders. For example, the Financial Institution Data Match program required by the Personal Responsibility and Work Opportunity Reconciliation Act of 1996 (PL 104-193) led to the location of 700,000 delinquent individuals being linked to accounts worth nearly \$2.5 billion.
- There were 378 million location searches used to enforce contractual obligations to pay debts.
- Tens of millions of searches were conducted by pension funds (location of beneficiaries), lawyers (witness location), blood donors organizations (blood supply safety), as well as by organizations focused on missing and exploited children.

Clearly our members are producing best-in-class data products and services that protect consumers, prevent crimes, mitigate risks and enable robust competition. US laws governing the flow of consumer data, such as the Gramm-Leach-Bliley Act and Fair Credit Reporting Act, are protective of consumer rights and also ensure that products used to protect consumers, prevent fraud and to locate individuals are allowed to operate for the good of consumers and business.

DATA FLOWS AND THE FUTURE

While some may think that the United States has been trying to catch up to the world when it comes to data flows and regulation, this is not the case. Well prior to the first OECD Fair Information Practices Guidelines of 1980 or any action taken by the European Union our country had enacted the Fair Credit Reporting Act which regulates

all third-party aggregated data used for making a decision about a consumer. Congress was prescient in this action. As discussed above our sector-by-sector approach to laws and regulations has not resulted in a dearth of protections for consumers or congressional oversight. Where laws have been needed congress has passed them. In fact there is an extraordinarily thorough record of congressional oversight of various industry sectors' uses of personal information. The U.S. has chosen a sector-specific structure to consumer data laws which ensures regulatory structures which are both appropriate to the data and which can be effectively enforced. Sector-specific laws and regulations exist today because of such oversight and due to the expertise of different committees overseeing different aspects of American business.

What is also clear is that there is not a homogeneous world view when it comes to how consumer data protection should be structured and one cannot turn to Europe with the assumption that their work is a reflection of world opinion. There have been many different approaches to establishing basic principles for the protection of data including just a few of the many listed below:

- The 1973 HEW Report contains 5 principles.
- The 1980 OECD Guidelines contain 8 principles.
- The 1995 EU Data Protection Directive contains 11 principles.
- The 2000 FTC Report on Online Privacy contains 4 principles; and
- The 2004 APEC Privacy Framework contains 9 principles.

Even in Europe the Data Protection Directive has been transposed into country-specific laws which, while perhaps determined as adequate by the EU, are still different. Today credit reporting is still a balkanized process that impinges on the theory of a single market for financial services competition. Consumers who move from one country to another may find that their credit reports are not portable and thus they start over and all of their historical hard work in managing their credit is lost. This example alone argues against the theory that there is a single theory or right answer when it comes to how consumer data should be protected.

New reports by the FTC and the Department of Commerce introduce ideas into the U.S. dialogue but they are not offered as final conclusions. International commentators question whether or not the current U.S. discussion will ineluctably lead to the theoretically important aspirational goal of harmonization with other privacy conventions such as that of Europe. Consider the following comment submitted to the U.S.

Department of Commerce as indicative of this point:

“From a European perspective, it is not clear whether these provisions apply to personal data in the public domain. The document supports the APEC Framework (recommendation 6), but that Framework does not apply to public domain personal data.

This lack of clarity may create harmonisation difficulties re privacy matters and this position highlights one fundamental difference which helps explain why the USA’s view of “privacy” is not the same as the European understanding of “data protection”.”

CDIA's members operate on a global basis and are respectful of individual countries' traditions and values. Our members are the most successful companies in the world when it comes to producing data that protects consumers, allows for effective risk-management and which facilitate competition. Historical context, cultural mores, and much more drive an individual country's deliberations about how to protect its citizens' data and this is no less true here in the United States.

CDIA itself has participated in international task forces such as that recently hosted by the World Bank and International Bank of Settlements to work on international standards for credit reporting. This international dialogue recognized that standards operate above the particulars of various countries' legal regimes and necessarily so. It also recognized that trans-border data flows can be achieved outside of the ill-conceived theory of global harmonization of data protection.

The APEC discussions are yet again fundamentally demonstrative of the fact that the world actively seeks and finds ways to ensure international trade issues are addressed. Such regional trade discussions are respectful of national interests and law, while also exploring new answers to questions of how best to encourage our global economy to expand and benefit all involved.

CDIA offered its expertise to the Department of Commerce when it negotiated the Safe Harbor Agreement with Europe. Such dialogues demonstrate that there is no fundamental tension between preserving the importance of domestic laws that empower the U.S. economy and still finding a means of addressing the concerns of trading partner via mutually respectful discussions.

In closing, it is our view that our U.S. model has worked exceptionally well for our citizens and for our economy. We continue to support a sector-specific approach because:

- Laws resulting from this approach are far more likely to respect free speech rights in our constitution, an American value that cannot be subordinated to any external dialogue.
- Laws are more likely to be focused and overreaching in a manner that would impinge on innovation.
- Laws are subjected to the deliberations and oversight of congress which is obligated to represent the interests of the citizens of this country.
- Decisions about data protection are not an abrogation of congressional authority through the establishment of a new federal regulator with regulatory powers that overshadow on the legislative authority of the congress, itself.
- History has proven that our approach works well for our country and for our citizens.

Thank you for this opportunity to testify and I am happy to answer any questions.