STATEMENT OF STUART K. PRATT

CONSUMER DATA INDUSTRY ASSOCIATION

WASHINGTON, D.C.

Hearing on

"Personal Information Acquired by the Government from Information Resellers: Is There Need for Improvement?"

Subcommittee on Commercial and Administrative Law

and

Subcommittee on the Constitution

Committee on the Judiciary

United States House of Representatives

Washington, D.C.

Tuesday, April 4, 2006

Chairmen Cannon and Chabot, Ranking members Watt and Nadler, and members of the committees, thank you for this opportunity to appear before you today. For the record, my name is Stuart Pratt and I am president and CEO of the Consumer Data Industry Association.[1] Our members appreciate this opportunity to discuss our serious concerns with basic premises which underlie and methodologies employed in drafting the report written by the General Accountability Office (GAO) regarding the government's use of data provided by consumer data companies.[2]

THE RECOGNIZED VALUE OF CDIA MEMBERS' SYSTEMS

CDIA's members are the leading companies producing consumer data products and services for both the private and public sector markets. The GAO report surveys governmental uses of our members' systems, but leaves the reader with a less than complete perspective on the value and effectiveness of such services. Consider the following examples of governmental uses of our members products and services:

- Preventing money laundering and terrorist financing through investigative tools.
- Enforcing child support orders through the use of sophisticated location tools.[3]
- Assisting law enforcement and private agencies which locate missing and exploited children through location tools.

[1] CDIA, as we are commonly known, 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.

[2] The GAO employs the term information reseller and we have concerns with the use of the term which will be discussed later in this testimony. For example we do not believe that the term "consumer reporting agency" as defined by the Fair Credit Reporting Act should be commingled with other data products due to the specificity of law which regulates this product. The GAO fails to draw this distinction in its draft report.

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

- 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 effectively target manpower resources.
- Witness location through use of location tools.
- Entitlement fraud prevention, eligibility determinations, and identity verification through fraud prevention data matching and analytical products.
- Background screening for employment and security clearances.
- Disaster assistance.

Homeland security, law enforcement and entitlement program management are all faced with extraordinary challenges in accomplishing their missions. The GAO's report does not properly set the stage for understanding how difficult it is to accomplish their missions. Consider the facts regarding simply identity verification:

Personal identifiers change:

While it probably doesn't occur to most of us, the identifiers we use in everyday life do change and more often than most might think. For example, data from the U.S. Postal Service and the U.S. Census confirm that over 40 million addresses change every year. More than three million last names change due to marriage and divorce. While trends in naming conventions are changing, this fact is still far more often true for women than men.

We use our identifiers inconsistently:

It is a fact that we use our identifiers inconsistently for a wide variety of reasons. First, many citizens choose to use nicknames rather than a given name. However, there are times where, in official transactions, a full name is required, Some consumers, when hurried, use an initial coupled with a last name, rather than their full name or nickname. Consumers are also

inconsistent in the use of generational designations (e.g., III, or Sr.). Finally, there are times where consumers themselves do make mistakes when completing applications, such as transposing a digit in an SSN. Thus, a consumer's identifiers may be presented in different ways in different databases and, in some cases, the data may be partially incorrect.

Personal identifiers are not always unique:

We think of our names as a very personal part of who we are. However, our names are less uncommon and unique than we might think. For example, families carry forward family naming conventions leading to some consumers sharing entirely the same name. Further, U.S. Census data shows that both first and last names are, in some cases amazingly common. Fully 2.5 million consumers share the last name Smith. Another 3 million share the name Jones and more than thirteen million consumers have one of ten common last names. First names are also used very commonly leading to common naming combinations. Eight million males have either the name James or John and a total of 57 million males have one of ten common first names. An additional 26 million females have one of ten common first names. Common naming conventions make it more difficult and in some cases impossible to depend on name alone to properly match consumer data.

Identifiers are shared:

Our birthday is a unique day in our lives, but it is, nonetheless, a date shared with hundreds of thousands of others. Date of birth alone is not an effective identifier. Family members who live together end up sharing addresses and per our discussion above, where consumers share the same name due to family traditions and the address at which they live, distinguishing one consumer from another is complex.

Data entry errors do happen:

Hundreds of millions of applications for credit, insurance, cellular phone services, and more are processed every year. There is no doubt that in the process of entering a consumer's identifying information errors can be made which carry forward into databases and into the reporting of data to consumer reporting agencies.

We do not always update our records:

Consumers don't always remember to update records when they move or when portions of their personal identifying information change. For example, consumers are permitted to change their social security number under certain circumstances in addition to officially changing their names and while the percentages of consumers who take these steps is small relative to the U.S. population, such changes do affect data matching systems. It is important to know that some consumers try to separate themselves from their records on purpose and apply with the SSA for employer ID numbers (EINs) to use in lieu of their SSNs.[4] A non-custodial parent who does not want to pay child support might employ such tactics in order to avoid being located and forced to fulfill a court order. A consumer who does not want to take responsibility for their mismanagement of credit and hopes that by using new identifying to separate himself/herself from a credit report is another example. Clearly fugitives are another example of a type of person who will employ tactics to try and separate themselves from their histories.

These facts about our identifying information demonstrate how challenging it is to match records with individuals and why the products, tools and services of our members are in such high demand.

[4] The FTC investigates "file segregation" schemes. Here's what they say on their website about this activity: "You're promised a chance to hide unfavorable credit information by establishing a new credit identity. The problem: File segregation is illegal. If you use it, you could face fines or even a prison sentence."

Let's now consider what government representatives themselves have said about the value they derive from the use of consumer reporting agencies and other consumer data companies. On September 8, 2005, the Department of Homeland Security held a workshop which explored its use of commercial data. This public meeting brought forward important input which informs the record of this hearing.

Regarding identity verification, Grace Mastalli, Principle Deputy Director for the Information Sharing and Collaboration Program in DHS stated the following regarding the value of CDIA member services: "There are people without prescriptions, without driver's licenses, and it the commercial data sources, in many instances right now, that are facilitating not just placing people, but verifying their identities to the claims…we get to make sure that entitlements go to individuals who deserve them."

Regarding how our members' systems contribute to the accuracy of governmental systems, Mastalli indicated that "we have sometimes used commercial data, not just to support identity authentication, but to assure the integrity of government data, and the accuracy of government data. Unfortunately, in many respects, the commercial enterprises have done better jobs of organizing and, what I call 'cleaning' data to eliminate errors in data."

Mr. Jeff Ross, senior advisor in the area of money laundering and terrorist financing, in the Office of Terrorist Financing and Financial Crime at the Department of Treasury, also participated in this DHS workshop. He pointed out that many crimes have a financial aspect to

them including narcotics trafficking, public corruption, terrorist financing, and organized crime in general. His comments help explain the investigative research value of CDIA member tools where he states "so commercial data bases are very important to us in law enforcement area to be used proactively…we have targets and need information, where you are trying, also, to find a specific individual or entity that should be involved….who could also be potential witnesses in a case."

Mastalli provided a very concrete example of how the sophistication of private-sector data matching tools contributes to efficient use of governmental law enforcement agents. She noted that "…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 to eliminate the 17 instances of an individual who has a phonetically spelled name being recorded as 17 people instead of one." She goes on to explain that government cannot always anticipate what data might be of value to a particular investigation. Mastalli provided the following scenario: "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. One of the issues here is that, other than the name of the owner or manager of scuba diving schools, there was no personally identifiable data."

To further the point regarding the value of commercial data our members supply, consider the following two examples:

Example 1:

In this example we learn how the aggregation of public records creates low-cost research efficiencies that ensure that "shoe leather" investigations conducted by highly trained personnel are truly are targeted and results-focused. 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.[5] 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.[6] 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.[7]

Example 2:

While this next example is drawn from the private sector, it helps illustrate how fraud prevention

[5] http://www.choicetrust.com/servlet/com.kx.cs.servlets.CsServlet?channel=home&product=bgcheck&subproduct=default&anchor=#. All RVI providers recommend that employers should supplement 'no criminal record found' results with a local county records search before making a hiring decision as any national criminal database will not contain all current criminal records since courthouses add new records daily.

[6] Id.

and identity verification services reduce fraud and is analogous to the value of such systems when used by the government, as well. 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.

The GAO paper should have done more to speak to the value of the commercially available data and analytical tools our members provide and not merely to provide an accounting of governmental uses. We hope that the above discussion will inform the this hearing record and set a more complete context for these committees' future deliberations.

CONCERNS WITH GAO'S REPORT

Now having an appropriate context for truly understanding the value that our members' services bring to both the public and private sectors, I would like to discuss serious concerns we have with the GAO's presentation of current Federal laws and how they regulate our members' practices as well as their attempt to apply the 1980 Organization for Economic Development (OECD) privacy guidelines to the practices of "information resellers." We believe that a thorough understanding of the decades of congressional oversight and action is essential to today's hearing.

The State of Current Federal Laws

[7] Assuming each in-person search costs $16, the same as an in-person county courthouse search.

The United States is on the forefront of establishing sector-specific and enforceable laws regulating uses of personal information of many types. The GAO does provide an accounting of some of these Acts on page 18 of their draft report. Their accounting includes the Fair Credit Reporting Act (15 U.S.C. 1681 *et seq.*)[8], 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.*).

While the GAO relegates their discussion of statutory requirements to Appendix II of the draft report, we believe that such a discussion is essential and that it should have been included in the body of the report. In doing so, the GAO would have provided readers with a better one-to-one understanding of the operation of current laws in contrast with their views of the application of OECD guidelines US information practices.[9] For example, it is important to note that, predating 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, was enactment of the Fair Credit Reporting Act in 1970. Equally important is understanding the breadth of the application of this law in particular and thus why a discussion of consumer data companies in general should not be commingled with a discussion of the practices of consumer reporting agencies.

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

[8] The GAO also lists the Fair and Accurate Credit Transactions Act of 2003 (Pub. L. cite), however this act is in fact a series of amendments to the FCRA.

discussion. It has been the focus of careful oversight by the Congress resulting in significant changes in both 1996[10] and again in 2003.[11] There is no other law that is so current in ensuring consumer rights and protections are adequate.[12]

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 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[13], 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. Again, this law applies equally to governmental uses and not merely to the private sector.

Because personal information about consumers is used for decisions to accept or deny access to a

---

[9] CDIA has serious concerns about the attempt by the GAO to measure the acceptability of the practices of US consumer data companies, which are in fact regulated by US laws today. This concern will be discussed more fully later in this testimony.

[10] See Pub. L. 104-208, Title II, Subtitle D, Chapter 1).

[11] See FACT Act Amendments (Pub. L. 108-159).

[12] It is also true that the Gramm-Leach-Bliley Act, Title V provisions regulating the use of nonpublic personal information is current due to the extensive role that federal banking regulators and the Federal Trade Commission play in drafting regulations, issuing guidance and enforcing the law.

[13] This includes national security investigations, background checks for security clearances, basic employment screening processes for new hires, review processes for promotions, and more.

consumer, they have fundamental rights which the GAO report does not discuss in any depth and which demonstrate why it is inappropriate to attempt to overlay a discussion of OECD privacy guidelines with this statute. 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 where there is suspected fraud, where a consumer is unemployed and seeking employment, 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. A separate GAO report produced

as a result of the FACT Act indicated that in a single year, perhaps 50 million consumers see their files and receive these notices.

- 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 the FTC and functional bank regulators.

The GAO report does not attempt to describe the delivery of products regulated under the FCRA and thus fails to properly inform the reader of the concomitant rights accorded in all of these cases. Every CDIA member mentioned in this report is operating, in part and sometimes solely as a consumer reporting agency. Therefore, in every case where products sold to governmental agencies were used for a determination of a consumer's eligibility, they were regulated by the FCRA with all of the rights discussed above. The GAO's report should have acknowledged this fact and discussed uses of consumer reports separately from other data products.

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, the sensitivity of the data, etc. Our members produce and sell a range of fraud prevention and location products which are governed by other laws such as GLB.

Fraud prevention systems deploy a diversity of strategies. In 2004 alone, businesses conducted 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.

Fraud detection tools are also known 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 public and private sector uses. 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 or are on terrorist watch lists, 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.

Who uses Fraud Detection Tools?

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.

Location services and products

CDIA's members are also the leading location services providers in the United States. These services, which help 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, but again, a key is the SSN. Consider the following examples of location service uses:

- There were 5.5 million location searches conducted by child support enforcement agencies to enforce court orders. Access to SSNs dramatically increases the ability of child support enforcement agencies to locate non-custodial, delinquent parents (often reported in the news with the moniker "deadbeat dads"). 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, as well as by organizations focused on missing and exploited children.

Clearly location services bring great benefit to consumers, governmental agencies and to businesses of all sizes.

CDIA CONCERNS WITH THE GAO'S USE OF TERM INFORMATION RESELLER

As discussed above, part our concern with the GAO's report is that it commingles a variety of different business models under a single term "information reseller" and in doing so the report

also commingles data products which are regulated under different Federal laws. For example, CDIA's members which are operating as consumer reporting agencies should not be discussed in the report as though they are not in fact highly regulated businesses. Similarly, CDIA's members which are defined as "financial institutions" under GLB are also highly regulated with regard to how information is to be used (see Section 502(e)) as well as though extensive federal agency rules prescribing how such information should be secured.

By employing the term "information reseller" readers are left with the wrong impression that such a term may exist in law or that it is possible to consider the multiplicity of different business models (and products produced therein) that make up the consumer data industry as a single type of entity and one that, in the eyes of the GAO, is not highly regulated. It is exceedingly difficult, if not impossible, to make meaningful statements which have the breadth of those often made in the draft report regarding the practices of many different types of business models delivering different products and services. Finally, we also strongly disagree with paper's attempt to simplify a discussion of our members' businesses which are in fact highly regulated under a variety of sector-specific laws by attempting to apply a set of OECD guidelines as though there are not laws which were thoroughly debated by the congress over the years and which are mature and protective of consumer's today.

CDIA CONCERNS WITH GAO OECD GUIDELINE APPLICATION

Let me amplify on our concerns regarding how the GAO has attempted to apply the 1980 OECD privacy guidelines as a scorecard against which to evaluate the practices of CDIA members.

Due to the GAO's mistaken assumptions about the breadth of the application of current laws, the GAO also makes the mistake of thinking that a fair information practices framework can operate as a one-size-fits-all yardstick. We disagree for a variety of reasons.

First, we are concerned about how the GAO attempted to make use of the guidelines. Let us consider what the OECD said about their own guidelines:

> *These Guidelines should not be interpreted as preventing:*
>
> *a) the application, to different categories of personal data, of different protective measures depending upon their nature and the context in which they are collected, stored, processed or disseminated;*

Further to the question of how privacy guidelines are to be used, in the 1977 Report of the U.S. Privacy Protection Commission it was noted that "[P]rivacy, both as a societal value and as an individual interest, does not and cannot exist in a vacuum….[T]he privacy protections afforded [to societal relationships] must be balanced against other significant values and interests. It is very common to find such statements associated with guidelines because they are not considered to be definitive rules with equal applicability to all data flows. We do not believe that the GAO's report adheres to this guidance provided by the authors of the OECD guidelines themselves or fully accounts for the U.S. Privacy Commission's admonition regarding how to apply guidelines.

Second, the GAO suggests, not purposefully, of course, but by omission that there is a single global opinion regarding which set of guiding principals is preeminent. To the contrary, consider the following:

- 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.

Each framework has to be applied with care and not monolithically across all data uses however different they may be in terms of risk, use, content and so on. The GAO does not explain why a particular set of principles was chose and as previously stated, we believe that the GAO's methodology by which the OECD principles was applied is flawed.

Third, as discussed above, 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. The GAO, by implication and likely unintentionally, implies to the reader that all such oversight was incomplete and that a single evaluative standard is the right approach to analyzing our members business models and products. This, however, is a very fundamental flaw in the GAO's approach. Sector specific laws ensure that they are tailored to the industries, to the uses of data and to the risks involved. How healthcare data (i.e., HIPAA) is regulated is inevitably different than how one might regulate a telephone number (i.e., Do Not Call). Ultimately, tailored laws and regulations ensure that consumers are

protected, but also are empowered by the data about them.

Fourth, the GAO's one-size-fits-all approach to applying the OECD guidelines ignores a fundamental bifurcation that exists with regard to information use and that is the difference between consumer data products used for eligibility determinations and those which are not. A fraud prevention product, for example does not end a transaction, but provides a user with a "caution flag" which encourages the user to take additional steps to further authenticate a person's identity. As discussed above, where data is provided by our members for eligibility determinations such as employment or credit, the FCRA already provides a robust set of rights and protections for consumers. Regulation of consumer data where it is used for eligibility determinations is different than regulating consumer data used for fraud prevention or investigative location tool used by law enforcement. By not accounting for this essential bifurcation in uses, application of the OECD guidelines leaves readers with the wrong impression about how good data protection laws should operate.

Fifth, the GAO does not properly account for the system of public records which exists in our country and which has been considered a key pillar in the success of our democracy. Unlike other nations, our government cannot withhold information about us from us. Governmental transparency is achieved through open records and freedom of information acts at the state and federal levels. The application of many aspects of any one of a number of principles works against a system that has been in place since the early days of our country's existence. The GAO's report does readers a disservice by not discussing the unique nature of public records and by attempting to apply the OECD guidelines to this system of records.

To amplify on our general concern about the GAO's approach to applying OECD guidelines, let's now consider some specific illustrative examples.

Consumer Consent

The report states that "[r]esellers generally do not adhere to the principle that, where appropriate, information should be collected with the knowledge and consent of the individual."[14] The reader is left with the wrong impression regarding the practices of our members, the laws which currently regulate them and the appropriate application of a consent standard. For example, the GAO does not attempt to apply a consent-based standard on a product specific basis or even a business-model-specific basis, which is an inherent flaw in their methodology. If one were to apply such a standard to, for example, consumer credit reports, then the result would be to give consumers the ability to pick and choose which creditors' data would be reported to a credit bureau. Consumers could allow creditors they intend to pay on time to report and could prohibit from reporting those that they don't intend to pay on time or at all. The result would be to turn the nation's credit reporting system on its head and to affect the fundamental safety and soundness principle upon which our banking system has operated since the days of the great depression. In 1970, Congress recognized the inapplicability of this fair information practices concept since it would essentially work against the fundamental premise of data acting as an independent affirmation of a consumer's own willingness to pay, or otherwise qualify for a benefit. In a second example, of what value would an identity verification tool be if consumers who intend to commit fraud can decide which data will or won't be used? A third example involves public records. How does one apply a consent standard to records which are in the

[14] Page 44, Draft Report.

public domain? Through these examples, it is clear that consent is not a universal concept which can be applied to all data flows.

Data Quality

The title of the data quality discussion is "Information Resellers Do Not Ensure the Accuracy of Personal Information They Provide." This is misleading. As discussed above, CDIA's members are committed to the quality of information they collect. Further, in all cases where the data is used to produce a consumer report used for an eligibility decision, the standard for accuracy is found in the FCRA.[15] It is a standard that has been in place since 1970 (and amended extensively in both 1996 and again in 2003) and which applies to eligibility decisions such as applications for insurance, employment, government entitlements or credit. The GAO report does not properly acknowledge this fact or the breadth of the application of FCRA to consumer data transactions involving consumer reporting agencies. However, applying an accuracy standard to an investigative product used to locate individuals makes little sense. These location services are predicated on possible connections between addresses, names, etc., which are then followed up with direct contacts by law enforcement agents or collection agencies, for example. Location services are certainly high quality services and often are very precise, but since these products are not used to make an eligibility determination (e.g., job, credit) they are not regulated in the same way. This said, the quotes drawn included in this testimony regarding the high quality of consumer data products purchased by law enforcement or counterterrorism agencies (81% of users according to the GAO) speak for themselves. Like consumer consent, the concept of data quality cannot be applied in the same manner to each consumer data product as is implied

by the GAO's methodology.

Use Limitations

The GAO report states that "[r]esellers do not generally limit the use of information beyond those limitations required by law." It is not clear what the GAO intends by this, but in fact both Title V of GLB and Section 604 of the FCRA do, for example, impose significant limitations on the use of nonpublic personal information and consumer reports respectively. The GAO's report does not acknowledge these use limitations in the context of their discussion. Further the GAO does not state that use limitations cannot apply to public records which are not gathered for purposes under the FCRA since such records are generally available to the general public directly from Federal, state and local agencies and courts. This said, the Drivers Privacy Protection Act does impose use limitations on records coming from state motor vehicle agencies. The draft report also states that "[w]ithout limiting use to predefined purposes, resellers cannot provide individuals with assurance that their information will only be accessed and used for identified purposes." This criticism of the system of laws and contract is without basis. We have discussed the extent of the laws which impose a variety of use limitations and as evidenced by the GLB's service provider requirements (in effect since 2001), HIPAA's business associate requirements (in effect since 2003), and the concept of using contracts to limit use is an entirely appropriate system for consumer data companies. In fact many laws which restrict uses of information, also require that certifications through contracts be obtained.

Access and Correction

[15] The standard of accuracy in FCRA can be found at Sec. 607(a). A consumer reporting agency must use

CDIA's members when operating as consumer reporting agencies provide full access and a right of correction for all consumer reports. Consumer reports are used for eligibility determinations and thus our members fully agree with the application of this principle. However the application of an access and correction principle applied to a fraud prevention and location data base would result in empowering criminals to delete information that is used for pattern analysis and other analytics which help in linking suspects or key pieces of information necessary to stop fraud or to solve a case. The GAO's report does not properly describe the harmful application of an access and correction regime to location, investigative and fraud prevention systems which are not used to stop a transaction or prevent a consumer's access to a service or benefit (eligibility). In fact FTC Chairman Majoras stated in a letter responding to questions about the imposition of an access and correction obligation on information resellers:

> *"Before extending this approach to additional databases [beyond FCRA], however, it is necessary to consider carefully the impact of such extension. For example, requiring data merchants to provide consumers with access to sensitive information may itself present a significant security issue – in some cases it may be difficult for the data merchant to verify the identity of someone who claims to be a particular consumer demanding to see his or her file. Similarly, for databases that are used to prevent fraud or other criminal activities, providing correction rights could pose serious problems; those trying to perpetrate the fraud may take advantage of the right to 'correct' data to hide it from those they are trying to defraud."*

---

reasonable procedures to assure the maximum possible accuracy of the information in the report.

The GAO report states in its conclusion that "[g]iven that reseller data may be used for many purposes that could affect an individuals livelihood and rights, ensuring that individuals have an appropriate degree of control or influence over the way in which their personal information is obtained and used – as envisioned by the Fair Information Principles – is critical." For all of the reasons discussed above, the GAO has failed to support this claim because:

- Their analysis does not properly account for the severe regulation of consumer reporting agencies, and the breadth of the FCRA's application to all eligibility transactions which apply to all governmental transactions and uses.
- In taking a one-size-fits-all approach, the analysis does not properly account for the destructive consequences of applying various principles in the same way to all business models and product which make up the consumer data industry.
- In making this claim, the GAO often ignores or undercuts decades of congressional oversight, legislative enactments (FCRA, GLB, HIPAA, DPPA, etc.), federal regulatory activities and law enforcement actions.

CONCLUSION

In conclusion, the members of the CDIA believe that the GAO's report is methodologically flawed and often misleads readers through the attempt to apply a once-size-fits-all analysis of a set of privacy guidelines. The consumer data industry does not consist of a single entity called an "information reseller." It is an industry with a diversity of business models focused on the production of consumer reports, fraud prevention tools, location and investigative products, analytics services and more. CDIA's members create incredible value for the government agencies which use their services. 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 to complying each and every day.

We appreciate this opportunity to testify and we welcome your questions.