

Privacy and Public Land Records: Making Practical Policy

A White Paper by the Property Records Industry Association



**P.O. Box 3159, Durham, NC 27715-3159
919.433.0121**

**PRIA Copyright Notice, Disclaimer and End-User License
Version 1.1 November 2003 (the “PRIA License” or the “License”)**

This document or software (the “Work”) is published by the Property Records Industry Association (“PRIA”). Copyright © 2006, Property Records Industry Association. All rights reserved.

Subject to this License, Licensor hereby grants any user of this document or software (“Licensee”) a worldwide, royalty-free, irrevocable, perpetual, non-exclusive license to reproduce the Work in copies, to prepare proprietary derivative works based upon the Work, to distribute copies of the Work to the public by sale or other transfer of ownership, and to display the Work publicly.

Any distribution of copies of the Work, or of a derivative work based upon the Work, shall reproduce verbatim the above copyright notice, the entire text of this License and the entire disclaimer below under the following header: “This document includes works developed by PRIA and some of its contributors, subject to PRIA License, Version 1.1 November 2003 published at www.pria.us/license.htm or any subsequent applicable version of such License.” Any software application developed by Licensee based upon the Work shall include the following notice in its end user documentation and in its codes: “This software product includes software or other works developed by PRIA and some of its contributors, subject to PRIA License, Version 1.1 November 2003 published at www.pria.us/license.htm or any subsequent applicable version of such License.” Upon publication of a derivative work, Licensee shall inform PRIA of such publication and address to PRIA a copy of Licensee’s derivative work and any relevant documentation.

“PRIA” is a trade name of the “Property Records Industry Association.” No derivative work or altered versions of a Work by Licensee may be trademarked or labeled in reference to PRIA or any of its trademark(s) or service mark(s) without PRIA’s prior written approval. No reference to PRIA or any of its trademarks by Licensee shall imply endorsement of Licensee’s activities and products.

DISCLAIMER: THIS WORK IS PROVIDED “AS IS.” PRIA, THE COPYRIGHT HOLDER, THE AUTHORS OF THIS WORK AND ANY STANDARD -SETTING BODY CONTRIBUTORS TO THIS WORK MAKE NO REPRESENTATIONS OR WARRANTIES (i) EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE OR NON-INFRINGEMENT; (ii) THAT THE CONTENTS OF SUCH WORK ARE FREE FROM ERROR OR SUITABLE FOR ANY PURPOSE; NOR THAT IMPLEMENTATION OF SUCH CONTENTS WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. IN NO EVENT WILL PRIA, THE COPYRIGHT HOLDER. ANY AUTHOR OF THIS WORK, OR THE STANDARD-SETTING BODY CONTRIBUTORS TO THIS WORK BE LIABLE TO ANY PARTY FOR ANY DIRECT, INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES FOR ANY USE OF THIS WORK, INCLUDING, WITHOUT LIMITATION, ANY LOST PROFITS, BUSINESS INTERRUPTION, LOSS OF PROGRAMS OR OTHER DATA ON YOUR INFORMATION HANDLING SYSTEM OR OTHERWISE, EVEN IF PRIA, THE COPYRIGHT HOLDER AND/OR ANY AUTHORS AND/OR ANY STANDARD-SETTING BODY CONTRIBUTORS TO THIS WORK ARE EXPRESSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

This White Paper is provided for educational purposes only. This Paper is not intended to substitute for professional advice. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

TABLE OF CONTENTS

OVERVIEW 1

OBJECTIVES 2

LIMITATIONS 2

PRIA ACTIVITIES TO DATE 3

INTRODUCTION TO ISSUES 4

OVERVIEW OF PUBLIC RECORDS 7

A MATTER OF RIGHT 7

PURPOSE OF PUBLIC RECORDS 7

 Integrity of Government and the Political Process 7

 Law Enforcement and Public Safety 8

 Information in the Public’s Interest 9

 Real Estate Transactions 9

 The Economy and Global Marketplace 10

THE COMMON LAW RIGHT OF ACCESS 10

STATUTORY PUBLIC RECORDS LAWS 11

FORM OF PUBLIC RECORDS 12

COMMERCIAL REQUESTORS 13

IDENTITY THEFT 14

 Understanding Identity Theft and Its Causes 15

 The Role of Public Records in Combating Identity Theft and Fraud 16

 Balancing Security with Access 16

DISCUSSION POINTS 16

PROHIBITING COMPLETE SOCIAL SECURITY NUMBERS ON PUBLIC LAND RECORDS
 17

 Availability of Social Security Numbers 17

 Privacy Focus: Social Security Numbers 17

 Redaction and Truncation of Social Security Numbers 18

 Narrowing False Positives 20

 Legitimate Business and Government Uses of the Social Security Number 20

 Balancing Benefits Versus Abuse of Public Records / Access to Social Security Numbers 23

ENACTED LEGISLATION CONCERNING SOCIAL SECURITY NUMBERS AND
 PERSONAL INFORMATION 24

 New Jersey 24

Texas	25
California	26
RECOMMENDATIONS.....	27
<i>CONSIDERATIONS FOR STATE AND FEDERAL LEGISLATION.....</i>	<i>27</i>
<i>PROPOSED ELEMENTS FOR SOCIAL SECURITY NUMBER MODEL LEGISLATION.....</i>	<i>28</i>
Legislation Should be on a “Day-Forward” Basis.....	28
Immunity of Recorders	29
Authority to Redact Post Effective Date.....	29
Voluntary Redaction by Public Prior to Delivery for Recording	30
Recorders Not to Redact Information from Documents to be Recorded.....	30
CONCLUSION	31
APPENDIX I.....	32
APPENDIX II.....	35

OVERVIEW

The hottest buzzwords of the first years of this new millennium include “Identity Theft” and “Personally Identifiable Information.” Congress, state legislatures, consumers, private businesses and public records custodians all wrestle with the best solution to the problem of protecting individual privacy rights while at the same time encouraging commerce and improving compliance with government regulations.

When serious consideration is given to the various facets of this topic, it quickly becomes clear there is no easy, “one-size-fits-all” solution. There is little disagreement that something needs to be done to counter the abuses that undermine faith in existing institutions, such as land recording.

As the standard-setting body for the land records industry, the Property Records Industry Association (PRIA) has stepped forward to facilitate frank and open discussion regarding traditional practices and emerging technology within the land records industry. As these emerging technologies are developed, the need to consider the possible or potential factors regarding identity theft, and identity fraud, using public records has grown.

This document is a project undertaken by PRIA to foster education and informed practical policy-making with regard to privacy and the public land records system.

The Privacy Access WorkGroup
The Records Access Advisory Policy Committee
Property Records Industry Association

OBJECTIVES

The goal of this White Paper is to outline some of the key issues faced by the land records industry and to recommend some “best practices” and legislative initiatives.

We will explore the history of the public land records system to ensure that our discussions and recommendations are informed by the foundational elements that have made the American land records system a cornerstone of the world’s most successful economy.

We will discuss the importance of access to public records as well as the ever-increasing problem of identity theft. We will also address how public land records may be misused by those intent on committing identity theft as part of land fraud schemes.

PRIA has hosted two national forums, dedicated several sessions during conferences, and moderated an email listserv focused on this topic. This document will report on the consensus that has evolved from these various discussions.

We will conclude with our recommendations for best practices within our industry and legislative initiatives that we believe will ensure access while addressing the concern regarding the misuse of land records for identity theft activities. Some recommendations will apply to consumers, some will apply to land records custodians, and others will apply to document drafters who create documents destined for submission to public land recording offices.

LIMITATIONS

As we have already noted, no single solution can be applied effectively across-the-board to all industries or even all government agencies. This document will limit its scope to public land record offices only. However, it is important to understand that any discussion of these issues crosses over to public records in general.

We are aware that in some jurisdictions land records are maintained in an office dedicated solely to that purpose, while in other jurisdictions these records are administered as part of an office that also has custody of court records, birth/death records (vital records), or even election records. In multi-function offices, it is our intent to apply these recommendations to the land records department only.

Furthermore, we stipulate at the outset that a certain amount of “personally identifiable information” must be contained in the public land records system for the system to function properly. Clearly, the names of parties along with the address and/or legal description of the property, together with certain information specific to the property, and signatures must be included in real estate documents in order for state and county officials, and the public, to know who has an interest in what real property. Our discussion of personally identifiable information therefore, will be focused on social security numbers on real estate documents.

PRIA ACTIVITIES TO DATE

PRIA began seriously engaging the issue of social security numbers appearing in real estate documents in early 2003. As part of its Winter Conference in March 2003, PRIA hosted a “Privacy/Access Roundtable” in Washington DC. At the conclusion of the Roundtable, PRIA moved to establish a Privacy/Access Workgroup. The workgroup initiated an email listserv discussion around a number of privacy-in-public-records topics. Those discussions led to various presentations and open forum sessions at PRIA conferences in 2003 and 2004.

PRIA’s work in facilitating discussions regarding the inclusion of social security numbers in public documents gained the attention of members of Congress who were attempting to craft legislation to protect social security numbers from misuse. In July 2004, PRIA was invited to testify before the House Ways and Means Committee Social Security Sub-Committee regarding

HR 2971, the Social Security Number Privacy and Identity Theft Prevention Act of 2003 (see Appendix I).

Most recently, the use of social security numbers in real estate documents was a topic of discussion during the Financial Services Issues Forum hosted by PRIA during the Winter Conference of March 2005.

INTRODUCTION TO ISSUES

The issues surrounding privacy and public access to land records incorporate multiple, sometimes conflicting, ideals. Those ideals include proper operation and interoperation of federal, state and local governmental agencies, public and commercial access to the land records, privacy protection, and identity theft protection. One of the issues facing those whose task it is to manage land records is the availability of financial resources. Taking steps to prevent the disclosure of personally identifiable information often requires additional technology, software and services investment. Another issue is lack of understanding of the operational functionality of the land records management process in relation to both privacy protection and public access.

It is well-accepted that public records access is an essential component of our democracy. The government represents the people and thus public records are the people's records. With certain narrow exceptions, it is a matter of right in a democracy that the people – meaning everyone, without discrimination – have access to these records.

The importance of public records is usually thought of in terms of keeping the government accountable to the public and avoiding government secrecy. Another reason is economic. Reference to information contained in public records is either an absolute prerequisite for, or greatly facilitates, a number of different types of economic transactions, which are critical

to the country's economy. This is especially true for the various segments of the real estate industry, such as home mortgage lending.

Public records laws have been enacted by our federal government and by every state to ensure that government agencies uniformly, rather than selectively, apply these rights to every person. However, efforts to limit access to public records have been increasing in the past several years. In some instances, the restrictions address valid concerns, such as the restrictions on access to military discharge records filed for safekeeping with county agencies. Nevertheless, other restrictions can have the effect of eroding the foregoing principle and do more harm than good.

Property records recorded through the years sometimes have included personally identifiable information such as social security numbers, driver's license numbers, bank account numbers, dates of birth, etc. A number of other commonly filed documents, including federal tax liens and other governmental liens, child support liens, and court records, contain such personally identifiable information. This has caused a rise in concerns about their use in stalking, invasion of privacy, identity theft, and land fraud. These personal privacy issues are coming to the forefront in the land records world as we have migrated from paper to microfilm to digitized images to electronic documents, and have been making public information more readily available on the Internet.

Due to the escalating incidences of identity theft, often called the fastest growing crime in America, the public and our political leaders have become sensitized to the sources of information enabling identity theft. At this time, however, no reliable statistics or reports exist documenting any actual instances of identity theft occurring as a result of the availability of personally identifiable information in public records accessed by paper or over the Internet.

Nonetheless, heightened emotions and unawareness of the actual sources have caused, and may continue to cause, policymakers to react with decisions and proposed legislation that produce unintended consequences.

Some legislation, especially legislation that requires the redaction of personally identifiable information from previously recorded land records, requires (as mentioned above) the acquisition of additional software, and substantial labor or services investments on the part of public officials. However, how will this software, labor and services be paid for so as to avoid an unfunded mandate? Those who draft new legislation or who seek to modify existing legislation addressing privacy of personally identifiable information in land records should consider such costs and funding mechanisms for redaction technology.

The concerns relating to identity theft have resulted in new legislation at the state level. States including New Jersey, Texas, Florida and California have made efforts to address privacy protection of personally identifiable information with differing impacts on both business and government. This legislation is detailed later in this White Paper.

The Property Records Industry Association is very concerned about educating the public, the media, and policymakers about the benefits of land records, dispelling myths and misperceptions about their use, and keeping public records open to the people, to whom the public records belong. This White Paper provides information regarding the purposes of public records, the common law right of access, commercial requestors, and identity theft. Additional discussion is included regarding the prohibition of including complete social security numbers in public land records and recommendations for social security number model legislation.

OVERVIEW OF PUBLIC RECORDS

A MATTER OF RIGHT

A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives.

-James Madison

The above quote from James Madison epitomizes the importance of access to public records. It is a matter of right. It is a matter of empowerment . As eloquently stated by the District of Columbia Court of Appeals, in 1989:

The generation that made the nation thought secrecy in government one of the instruments of Old World tyranny and committed itself to the principle that a democracy cannot function unless the people are permitted to know what their government is up to.¹

PURPOSE OF PUBLIC RECORDS

Public records serve many valuable public purposes, ranging from providing the public with the information it needs to elect and monitor government officials to protecting the health, safety and security of citizens. Yet, many Americans are unaware that public records exist and, once known, most people rarely, if ever, contemplate the reason why public records are open.

Integrity of Government and the Political Process

Access to public records is central to electing and monitoring public officials and government operations, understanding the operation of the law, ensuring confidence in government, evaluating the cost-effectiveness and efficiency of government bodies, and protecting against illicit government activities. A person's ability to monitor the activities of local, state and federal government activities is as important as a person's right to vote.

¹ *Washington Post v. Minority Business Opportunity Commission*, 560 A.2d 517 (D.C. 1989).

Law Enforcement and Public Safety

Law enforcement officials rely on databases fueled by public record data to prevent, detect, and solve crimes. Each year, the FBI makes tens of thousands of inquiries to databases, enabling the agency to arrest fugitives, identify seizable assets, and locate witnesses. The type of databases and systems used by law enforcement are comprehensive and contain billions of records from across all 50 states.

For example, public record databases are used in efforts to find missing children. In the summer of 2002, police in South Carolina attempted to find information about Richard Evonitz, a man who had recently kidnapped and raped a 15-year-old girl. They contacted the National Center for Missing and Exploited Children. After searching a large public records computer database, the Center found a connection between the disappearance and deaths of three girls in Spotsylvania County, Virginia to the abduction of the girl in South Carolina. Using the information collected from the public records database that highlighted similarities between the two cases and attackers, the police acquired their biggest break in the Virginia case in years.

In 2002, public records databases played a key role in identifying and apprehending suspects in the Washington, D.C. area sniper shootings. Maryland police were able to access a database that cross-references billions of current and historical records, and make queries for possible suspects, as well as to trace the vehicle ownership to the suspects. The database used cross-referenced data such as addresses, phone numbers, driver's licenses, vehicle ownership, court records and property deed transfers.

In addition, such databases are also used to locate parents who are delinquent in making child support payments.

Information in the Public's Interest

Not only do journalists gather information about legislative proposals, government fraud and abuse, they also report on judicial decisions, crimes, waste and numerous other issues of importance to citizens. An open public record allows journalists to keep the general public abreast of important actions, issues and problems. For example, by systematically examining local government records, *San Francisco Examiner* reporter Candy Cooper discovered that police investigated rapes in upscale Berkeley far more readily than in the crime-infested neighborhoods of Oakland.

Other researchers, including journalists and non-journalists, use public information for thousands of studies each year concerning public health, traffic safety, environmental quality, crime, prisons, governance, and many other subjects.

Real Estate Transactions

Our entire system of real property ownership and nearly all real estate transactions depend on public records. These records are used to confirm the existence of the property, its location, its defined boundaries, its conveyance, and any other interests in the property. Real estate agents, brokers, appraisers, and multiple listing services, among others, all use public land records and information to perform their professional responsibilities within the industry. Buyers, lenders, title insurers, and others use these records to verify the title owner, track chain of title, and obtain constructive notice of liens and other impairments, which they would not otherwise be able to discover. Mortgages, many legal judgments, liens and other claims against real property require recording in the public record to notify anyone else interested in the property of rights against the property and its owners.

The Economy and Global Marketplace

The value of open public records extends beyond the democratic and social benefits outlined above. Public records have come to constitute part of the critical infrastructure of our information economy, which, in turn, contributes to the public good.

In order to grant credit rapidly and appropriately, the collection of information about consumers through public records is necessary for businesses to make fair and objective risk decision. Moreover, sustaining an open public record system helps reduce the cost of credit. This data is compiled routinely and efficiently instead of having to be assembled for each credit decision. Likewise, open public records help reduce consumer costs by preventing check fraud and identity theft.

THE COMMON LAW RIGHT OF ACCESS

The federal government and every state (including the District of Columbia) have enacted statutory public records laws,² generally beginning in the late 1960s through the early 1990s. However, even prior to the enactment of statutory public records laws, public records were still open under the common law right of access.³

A feature of the common law right of access is that the person seeking access is required to show a tangible interest. Stated otherwise, under the common law right of access, the burden is on the individual requesting access to a public record, rather than the other way around.⁴

² Public records laws of various jurisdictions are known by different names, such as the Freedom of Information Act, the Freedom of Information Law, the Public Records Act, the Public Information Act, the Open Records Act, the Right to Know Law, etc.

³ An excellent analysis of the common law right of access may be found in *Dugan v. Camden County Clerk's Office*, 870 A.2d 624, 376 N.J.Super. 271 (App.Div. 2005).

⁴ Interestingly, however, as explained in *Dugan v. Camden County Clerk's Office*, *supra*, the types and number of public records that may be obtained under the common law right of access are greater than

Furthermore, by the nature of common law (i.e., unwritten law), these standards can be ambiguous. As explained in the context of the U.S. Freedom of Information Act:

The Freedom of Information Act (FOIA) establishes a presumption that records in the possession of agencies and departments of the executive branch of the U.S. Government are accessible to the people. This was not always the approach to Federal information disclosure policy. Before enactment of the FOIA in 1966, the burden was on the individual to establish a right to examine these government records. There were no statutory guidelines or procedures to help a person seeking information. There were no judicial remedies for those denied access.

With the passage of the FOIA, the burden of proof shifted from the individual to the government. Those seeking information are no longer required to show a need for information. Instead, the “need to know” standard has been replaced by a “right to know” doctrine. The government now has to justify the need for secrecy.⁵

STATUTORY PUBLIC RECORDS LAWS

A foreseeable and predictable problem exists under the common law right of access; namely, that the identity of the requestor matters. In other words, a public official can very easily take the “I like this guy but I don’t like that guy” approach. Hence, the reason for the enactment of statutory public records laws: To *divest government officials of broad discretion* in determining what, if any, government records should be made available to the public upon receipt of a request for information.⁶

These principles have been restated in a number of public records laws which allow access to information about Government business. Examples include: Public information acts, freedom of information laws, and public records acts.

those available under the public records statutes, as public records statutes often contain a number of statutory exceptions to disclosure.

⁵ *A Citizen's Guide on Using the Freedom of Information Act and the Privacy Act of 1974 to Request Government Records* (H. Rpt. 106-50). Washington, D.C.: General Printing Office, March 11, 1999, at pages 2-3.

⁶ Senate Committee on the Judiciary, *Freedom of Information: A Compilation of State Laws*, Committee Print, 95th Cong., 2d Sess. (1978).

Pursuant to these principles, *every person*⁷ has a right to both access and receive a copy of a public record, *without regard to purpose*.⁸ By extension, most, if not all, public records laws do not contain any sort of restriction on what a requestor may do *after* receipt of the public record.⁹

In addition to the public records laws of each state, a particular type of public record may be addressed and open, under more than one statute. Real property records recorded with the county recorder or equivalent¹⁰ are an example, as some states have separate statutes (many of which predate the state's public records law) applicable to only county recorders.

FORM OF PUBLIC RECORDS

There are three different types of public records: Records of persons¹¹ interacting with the government (e.g. business licenses, voter registration records, criminal records), records and information about the business of the government (e.g. deliberations of legislative entities, meetings of government officials), and records of the transactions of a person maintained by the government (e.g. land records, DD-214 military records, deeds of trust, vital records, civil case records). These public records are maintained in many different forms. Most public records

⁷ Some states' public records laws contain a citizenship requirement, i.e., only citizens of the particular state are entitled to rights under the state's public records law. However, the majority of state public records laws do not contain any such limitation.

⁸ *See, e.g.*, California Government Code Section 6257.5 ("This chapter does not allow limitations on access to a public record based upon the purpose for which the record is being requested, if the record is otherwise subject to disclosure"). This principle has also been restated in a number of court or administrative decisions even in states where the irrelevancy of the requestor's purpose is not directly stated in the statute.

⁹ This is true under the common law right of access as well.

¹⁰ In some states, real property records are recorded with county clerks, county auditors, registers of deeds, etc.

¹¹ This use of the word "person" is as it is used in many statutes, that is to apply to both individuals and to other entities, such as businesses.

laws provide that a public record is public *regardless of form*. This means that it is irrelevant whether a public record is on paper, microfilm, tape, disk, or any other medium. It is still a public record.

Recognizing that many, if not most, of today's public records are maintained in electronic format, many public records laws also explicitly give the requestor the right to receive a copy of the public record in the electronic format maintained by the government agency.

COMMERCIAL REQUESTORS

The role of commercial requestors, such as public record information companies, has been vilified as of late, especially in connection with privacy concerns. The irony is that these companies serve a necessary business purpose. A public record information company obtains "raw data" from governmental agencies – the public records themselves. They then may add value to the data by analyzing, re-indexing, and amplifying the data to make it more searchable, among other things. Much of the business that is transacted in the United States is done with the help of public record information companies.

The foregoing is especially true in the real estate context. In particular, there are generally two methods of chain of title searching. One method is to search real property records directly at the applicable county recorder office. Another method is for a private concern to maintain an equivalent set of real property records – a "title plant" – and search the plant index and image databases at the title company offices.¹² With the title plant searching method it is no longer necessary to physically send a title searcher to the recorder's office.¹³ Searches can be

¹² See, e.g., Old Republic Title Company, "Methods of Title Searching," available at <http://www.oldrepublictitle.com/national/help/searching.asp>.

¹³ This benefits the recorders offices as well as their "traffic" is significantly reduced, freeing up time and resources.

performed when the information is needed, even outside of the recorder's normal business hours. This is why the title plant searching method has been in use in nearly all large metropolitan areas since the beginning of the title insurance industry.¹⁴

IDENTITY THEFT

Before the turn of the last century, one would have to take a ride on horseback to the county seat to pull the original Deed books to find information. This is the concept of “practical obscurity” of public records – personal information could be found in a public record, but there was little risk of harm to an individual because someone had to take the time to search the records at the recorder's office.

Technology undeniably has had a significant impact on access to public records. Technological developments raise concerns about how much information is too much information and whether there should be global access to public records.

It is a common misconception that easy access to public records has facilitated other types of fraud, identity theft, or land fraud. While posting documents that contain certain key information on the Internet, such as credit card numbers, social security numbers, and signatures, can provide a criminal with some of the information needed to commit identity fraud or theft, there is no evidence to support any claim that this is systematically being done to perpetuate identity theft crimes. There are many easier, and far more efficient, ways for identity thieves to obtain this information in today's world, as opposed to combing through public records and hoping to find something – a “needle in the haystack” approach.

¹⁴ “Methods of Title Searching,” *supra*.

That being said, a proactive approach to apply greater discretion to what public land record information is disclosed online is a reasonable approach to discourage the use of public land records to perpetuate identity theft and fraud. An accommodation between information privacy and access is appropriate and necessary.

Understanding Identity Theft and Its Causes

In September 2003, Synovate prepared the first ever Identity Theft Report for the Federal Trade Commission (FTC), based on interviews with 4,057 adults. In the report, identity theft was placed into three categories: New Accounts and Other Frauds' ID Theft, Misuse of Existing Credit Cards or Card Numbers, and Misuse of Existing Non-Credit Card Accounts or Account Numbers. The report did not identify a correlation between public records access and the three categories of identity theft.

New Accounts and Other Frauds' ID Theft are described as the use of one's personal information to open new accounts, take out loans and assume the identity of an individual. According to the FTC report, almost 3.25 million U.S. residents had their personal information stolen and misused in this manner in the preceding year.

The Misuse of Existing Credit Cards or Card Numbers totaled over five million victims in the preceding year and the Misuse of Existing Non-Credit Card Accounts or Account Numbers affected almost 1.5 million individuals. The misuse of existing accounts has the highest number of reported incidents, which might be explained by the improper disposal of banks records, credit card statements and paper records that people just throw away.

Evidence and testimony presented by the Chief Credit Officer of Household, Inc. before Congress showed that over half of all identity theft crimes are committed by family members or

business associates. This personal information is typically obtained from an individual's home or place of work.

The Role of Public Records in Combating Identity Theft and Fraud

It is important to understand that access to public records data is actually a very effective weapon in combating identity fraud and theft. Social security numbers compiled from public records (including court records) have proven to be the most reliable tool in verifying an individual's identity, which helps prevent the rapid increase in identity fraud victims. Commercial databases compiled using public records for identity authentication are routinely used to detect fraud, including credit card application fraud, insurance application fraud, and other types of fraud. Thus, efforts to restrict the collection and use of personal information contained in public records, though well intended, actually may hinder efforts to prevent identity theft by depriving businesses, government and law enforcement officials of valuable data that is used to authenticate identities and protect the public.

Balancing Security with Access

Federal, state, and local officials are tasked with the important challenge of both preserving the public's right to open government and with protecting citizens against identity theft and fraud. Several states have considered various approaches that are discussed below.

DISCUSSION POINTS

***PROHIBITING COMPLETE SOCIAL SECURITY NUMBERS ON PUBLIC LAND
RECORDS***

As states and localities look to enhance the privacy of their citizens, most are looking to prohibit the use and disclosure of an individual's social security number in public records. However, it is important to understand for which purposes and how social security numbers are used by government and the private sector, as well as what impact redaction and truncation have on record custodians, business, and the public.

Availability of Social Security Numbers

Forty-one states and the District of Columbia currently maintain at least one record that displays an individual's social security number, according to a U.S. Government Accountability Office (GAO) study conducted in November 2004. While social security numbers are displayed in various state and local records, the GAO study found that they were most often displayed in court and property records.

According to the study, state and local agencies responded that identity verification was the primary use for social security numbers maintained in public records, and that the primary method for inspecting such records was through paper copies. State and local governments reported that few records displaying social security numbers are available over the Internet and there were no plans to make them available in the future.

Privacy Focus: Social Security Numbers

A number of privacy advocates warn that the display of social security numbers in public records must be reduced as they are a primary piece of information in the commission of identity theft crimes. Given the nature of the social security number as a unique identifier for important

records and services, advocates are concerned that display of the numbers in public records makes it easier for identity thieves, both domestic and international, to obtain new credit and bank accounts in the names of their victims.

As outlined in the section entitled “Identity Theft,” at this time there does not appear to be any evidence supporting the claim that information derived from public records, including social security numbers, is systematically used to perpetuate identity theft crimes. That being said, it is reasonable to expect that government should, and must, institute reasonable safeguards to protect citizens from becoming victims of identity theft as a result of public land record abuse. This is addressed in the “Recommendations” section of this White Paper.

Redaction and Truncation of Social Security Numbers

Nearly every state legislature, and even the federal government, has considered legislation in recent years calling for the redaction or truncation of social security numbers contained in government public records. Several states have even passed social security number legislation. Moreover, at the writing of this White Paper, the U. S. Senate is considering The Personal Data Privacy and Security Act of 2005 (S. 1332, 109th Congress) and the Social Security Number Misuse Prevention Act (S. 29, 109th Congress).

The redaction of social security numbers from government public records involves the use of computer software to “block out” the offending data on a document so that is not visible on an electronic document, or on a paper document if the electronic document is printed. A person with certain security permissions can always retrieve the “original” digitized images which have not been redacted (See Appendix II for an overview of the redaction process).

It is reasonable to question whether social security numbers contained in a public record should be disclosed to the general public, since access to that information is generally not critical

to support the traditional and accepted uses of these records by the public. Businesses, however, rely upon accessing social security numbers from public records for a wide variety of purposes, which may ultimately benefit society and the economy.

Should there be two levels of access to public information: one for the general public, and one for other entities that demonstrate a tangible interest?

If the answer is yes, there remain other considerations, including what is a “tangible interest,” and who are the “general public?” There are also monetary limitations that most custodians of public records face which would prevent them from maintaining separate levels of access to the records they maintain.

Truncation of social security numbers raises an additional set of concerns. First, a truncated social security number does not necessarily provide individuals with enough security, since the social security number itself is constructed to reflect key information about an individual, namely where and when they received their social security number. This information could easily be obtained from other sources and combined with the final four digits, which are the only random numbers, to reconstruct the complete social security number.

The uses of social security numbers by industry are outlined in detail below, but it is important to understand that, generally speaking, truncation may impede the legitimate use of social security numbers in most cases but may also fail to provide the intended protection. In some instances, truncation will render the social security number useless for business purposes.

It is also important to consider the fact that collection, use, and verification of social security numbers is, in some instances, mandated by federal law. State and local efforts to limit the collection, use and verification of social security numbers could create a conflict between federal and state/local laws.

Narrowing False Positives

When the IRS began using social security numbers as a taxpayer identification number in 1961, employers and financial institutions were required to use the number for tax reporting purposes. In addition to other public record data, social security numbers help to narrow the incidences of “false positives” (the number individuals with identical or similar data elements) within important data records of individual citizens. Social security numbers are extremely helpful to citizens, state agencies and businesses in reducing false positives and in identifying the correct individual among a large pool of candidates with similar data attributes. Such ability to efficiently narrow false positives is critical for such instruments as property records, tax liens, and court records.

Legitimate Business and Government Uses of the Social Security Number

Preventing and investigating terrorist activities – The use of commercial databases is an important tool in protecting homeland security and our nation’s critical infrastructure. For example, information contained in commercial databases was instrumental in locating suspects wanted in connection with the September 11, 2001 terrorist attacks. The social security numbers contained in databases are a critical tool used by federal law enforcement agencies to locate suspects and witnesses, and to investigate and build cases against suspected terrorists.

Locating and recovering missing children – Locating a missing child within the first 48 hours is critical. After that time, the chance of recovering the child drops dramatically. In many of these cases, it is the noncustodial parent who has taken the child. The use of social security numbers is critical in locating the noncustodial parent and recovering the missing child.

Identifying and preventing fraud – Banks and other financial institutions routinely rely on social security numbers in public record information contained in commercial databases to detect

fraudulent credit card applications. Insurance companies have experienced similar successes through the ability to use social security numbers. The use of social security numbers in public records and other sources is key to preventing fraud.

Locating witnesses and helping make arrests – Lawyers are major users of social security numbers, which are critical to tracking down witnesses in connection with civil litigation, or heirs in probate matters. Law enforcement agencies also use commercial databases that contain social security numbers for homeland security purposes, to improve intelligence, and to aid in criminal investigations.

Preventing and investigating financial crime – Federal, state and local law enforcement rely on public records data to prevent and investigate financial crime. Similarly, industry has created tools using social security numbers that are used widely by banks and other financial institutions to screen new customers to prevent money laundering and other illegal transactions used to fund terrorist activities. The use of social security numbers by financial institutions to verify and validate information on prospective customers is critical to the success of this program.

Enforcing child support obligations and government assistance programs – Public and private agencies rely on social security numbers in public records and other information contained in commercial databases to locate parents who are delinquent in child support payments and to locate and attach assets in satisfying court-ordered judgments. Reliance on social security numbers contained in key public records is a critical component to the success of these searches. Additionally, government agencies use social security numbers in the administration of assistance programs to prevent or detect the fraudulent collection of benefits.

Helping locate pension fund beneficiaries – The task of locating former employees is becoming increasingly difficult. Americans move on average every five years, particularly when they change jobs. At any one time, about 20% of Americans are moving. Add to that the fact that an increasing number of Americans have two or more homes, often in two different states. Their names may change as a result of marriage or they may list slightly different names (*e.g.*, leaving out a middle initial) on employment documents. To ensure that pension fund beneficiaries receive the money owed them, plan administrators and sponsors are required by federal law to use commercial databases to search for missing pension beneficiaries. These services are by far the most cost-effective and efficient way to find these former workers. Pension Benefit Information, a leading service used to locate these workers, reported in public testimony delivered before Congress that searching with a retiree’s social security number results in an 85-90% success rate in locating an individual, compared to a success rate of only 8% without use of this information.¹⁵ Loss of access to social security numbers from public records by commercial locator services would dramatically increase the costs of locating former employees. Moreover, in many cases, employers would be unable to find former employees, resulting in a loss of pension benefits.

Helping locate blood, bone marrow, and organ donors – The National Marrow Donor Program and other similar programs use social security numbers to locate prior donors when someone with the same blood type needs a transplant. These programs also use social security numbers to locate individuals who have had bone marrow transplants in the past.

Contributing to important medical research efforts – Medical research centers use social security numbers to locate individuals who were past participants in their research programs.

¹⁵ Statement of Paula LeRoy, President, Pension Benefit Information, Tiburon, California, during testimony before the Subcommittee on Social Security of the House Committee on Ways and Means, May 22, 2001. <http://waysandmeans.house.gov/legacy/socsec/107cong/5-22-01/5-22lero.htm>.

Medical researchers also use social security numbers to estimate the year of birth and age for research subjects in occupational and epidemiological research where the social security number is known.

Notifying families about environmental hazards – Social security numbers are used by some environmental enforcement agencies to locate and notify individuals that an area in which they formerly resided has been identified as a hazardous waste area. Social security numbers are also used to identify, locate, and notify former workers of workplace exposure to hazardous materials.

Balancing Benefits Versus Abuse of Public Records / Access to Social Security Numbers

The federal government, states and businesses are either legally obligated, or choose to voluntarily control, the disclosure of records containing social security numbers. While privacy advocates call for greater control of access to social security numbers in public records, such a restrictive approach would threaten the ability of the government and businesses to accurately and efficiently verify the identification of citizens or consumers and authenticate that they are who they say they are.

Identity thieves are using a number of methods to obtain personal identification information, including “phishing” scams in which thieves send bulk or targeted emails to consumers impersonating legitimate businesses asking consumers to provide personal information such as social security numbers. “Phishing” has recently been expanded to include “spear-phishing.” “Spear-phishing” is where identity thieves send bulk or targeted emails falsely appearing as a commanding officer, in the case of military personnel, or as a superior or executive within an organization. These thieves ask that the employee email the supervisor or executive, at the false email address, their personal information to update records or to confirm

their personal information. Another new scam is “pharming,” where identity thieves redirect visitors from legitimate websites to “spoofed” websites (websites which look legitimate, but are not), and then collect personally identifiable information from these visitors.

It is important then that any legislative or regulatory attempts to restrict the access to, the display of, or use of social security numbers in public land records should carefully weigh the actual threat of identity theft with the efficient and current use of social security numbers in public land records by state and local governments, business and citizens.

ENACTED LEGISLATION CONCERNING SOCIAL SECURITY NUMBERS AND PERSONAL INFORMATION

Below are extracts of legislation that have been passed by New Jersey, Texas, and California concerning social security numbers and personal information. Florida has also passed social security number redaction legislation. In general, the legislation discussed below may not be perfect, but a model may be created through a combination of these examples (see Recommendations).

New Jersey

New Jersey’s public records law Title 47:1-16 (NJ AB 2047, signed into law in June, 2005) requires clerks to strike out social security numbers from documents to be recorded (as opposed to already recorded):

1. a. No person, including any public or private entity, shall print or display in any manner an individual's Social Security number on any document intended for public recording with any county recording authority.
- b. Whenever a document is presented for public recording with any county recording authority and that document displays a person's Social Security number, the recording authority shall delete, strike, obliterate or otherwise expunge that number prior to recording the document.

The fact that such a document is recorded without deleting, striking, obliterating or otherwise expunging that Social Security number shall not render the document invalid, void, voidable or in any way defective.

c. The provisions of this section shall not be applicable to a document originating with any court or taxing authority, any document that when filed by law constitutes a non-consensual lien against an individual, any publicly recorded document that is required by law to contain a Social Security number, or any document filed with or recorded by a County Surrogate.

d. The county recording authority shall not be liable for any claims arising from a violation of this act.

Note that these provisions apply on a “go-forward” basis, provide that a failure to comply shall not render the document in any way defective, and provide immunity for county clerks.

Texas

Another model is Texas Property Code Section 11.008, recently amended by SB 461.

This Section reads:

(a) In this section, "instrument" means a deed or deed of trust.

(b) Notwithstanding Section 191.007(c), Local Government Code, an instrument transferring an interest in real property to or from an individual and disclosing that individual's social security number or driver's license number must include a notice that appears on the top of the first page of the instrument in 12-point boldfaced type or 12-point uppercase letters and reads substantially as follows:

NOTICE OF CONFIDENTIALITY RIGHTS: IF YOU ARE A NATURAL PERSON, YOU MAY REMOVE OR STRIKE ANY OR ALL OF THE FOLLOWING INFORMATION FROM THIS INSTRUMENT BEFORE IT IS FILED FOR RECORD IN THE PUBLIC RECORDS: YOUR SOCIAL SECURITY NUMBER OR YOUR DRIVER'S LICENSE NUMBER.

(d) The county clerk may not under any circumstance reject an instrument presented for recording solely because the instrument fails to comply with this section.

(e) The county clerk shall post a notice in the county clerk's office stating that instruments recorded in the real property or official public records or the equivalent of the real property or official public records of the county:

(1) are not required to contain a social security number or driver's license number; and

(2) are public records available for review by the public.

(f) All instruments described by this section are subject to inspection by the public.

* * *

SECTION 3. The change in law made by this Act applies only to a deed or deed of trust executed on or after the effective date of this Act. A deed, mortgage, or deed of trust executed before the effective date of this Act is covered by the law in effect at the time the deed, mortgage, or deed of trust is executed, and that law remains in effect for that purpose.

* * *

It should be noted that Texas Property Code Section 11.008 specifically applies to real property records. The approach is to inform the individuals that they can remove social security numbers and driver's license numbers, prior to recording. This is different from the New Jersey model, where the clerks are directed to strike this information prior to recording.

California

The California Civil Code contains good existing provisions in connection with what "personal information" means and exceptions to display of personal information. In particular:

1798.81.5.

(d) For purposes of this section:

(3) "Personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

1798.82.

(f) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

1798.83.

(d) The following are among the disclosures not deemed to be disclosures of personal information by a business for a third parties' direct marketing purposes for purposes of this section:

(1) Disclosures between a business and a third party pursuant to contracts or arrangements pertaining to any of the following:

* * *

(D) Public record information relating to the right, title, or interest in real property or information relating to property characteristics, as defined in Section 408.3 of the Revenue and Taxation Code, obtained from a governmental agency or entity or from a multiple listing service, as defined in Section 1087, and not provided directly by the customer to a business in the course of an established business relationship.

Also, Civil Code 1798.85 provides, in relevant part:

1798.85. (a) Except as provided in subdivisions (b), (h), and (i), a person or entity may not do any of the following:

(1) Publicly post or publicly display in any manner an individual's social security number. "Publicly post" or "publicly display" means to intentionally communicate or otherwise make available to the general public.

* * *

(c) This section does not prevent the collection, use, or release of a social security number as required by state or federal law or the use of a social security number for internal verification or administrative purposes.

(d) This section does not apply to documents that are recorded or required to be open to the public pursuant to Chapter 3.5 (commencing with Section 6250), . . . of the Government Code. This section does not apply to records that are required by statute, case law, or California Rule of Court, to be made available to the public by entities provided for in Article VI of the California Constitution.

Note that the above provisions have served as model language in several non-California bills/laws, including, but not necessarily limited to, Texas, Missouri, New Mexico, and Illinois.

RECOMMENDATIONS

CONSIDERATIONS FOR STATE AND FEDERAL LEGISLATION

Prior to the development of state or federal legislation that affects the use of social security numbers and other data elements in public records policymakers should consider the following points:

- Before exempting any specific data element from collection by a government entity or from disclosure to the public, policymakers should first set out to

understand what records contain that data element and the reason for its presence in that record. Data elements are necessary in certain records and have a clear purpose. For example, without complete social security numbers in certain critical documents, such as tax liens, government and the private sector lose the ability to match data about individuals. Studying the potential impact of redaction or limits on collection of information is highly recommended *before* making any policy changes.

- Policymakers should solicit input from the custodians of the records and determine how a proposed policy will affect the records themselves as well as the ability of custodians to perform their duties.
- Policymakers must identify, or provide, funding mechanisms to carry out the redaction of public records so as to avoid an unfunded mandate. In this regard, a “go forward” recording fee for creating electronic versions of all recorded documents could be used to carry out the redacting process as well.

PROPOSED ELEMENTS FOR SOCIAL SECURITY NUMBER MODEL LEGISLATION

Legislation Should be on a “Day-Forward” Basis

Any legislation impacting a governmental agency’s acceptance, redaction, or truncation of documents which contain social security numbers should be effective on a “day-forward” basis only. This means that any legislation should not require redaction or expungement of records already filed or recorded (See Appendix II for an overview of the redaction process).

In particular, recorders will be faced with a nightmarish task of redacting records that are already filed, or recorded, including those in other mediums such as microfilm or microfiche.

Changes to the permanent official record require constant updating of archival copies and on security copies maintained by the recorder. Tracking these updates can be a management headache and an additional source of liability for the recorder who is trying to maintain the current versions of the permanent official record, archive records, security copies, and websites.

Depending on the method used for redaction, the recorder may be faced with managing two databases or two sets of redacted documents. It is possible that mistakes or omissions could occur in the public record if recorders are required to manage and maintain two sets of databases, or redacted and unredacted images. Redaction of official records and updating archival and security copies could mean having to delve into technology or methods of preservation that are no longer available to the recorder or archiving facility.

Immunity of Recorders

Recorders are custodians, or stewards, of the information they are required by law to maintain. It should be the responsibility of document preparers and individual consumers, and not recorders, to make sure that documents presented to recorders for recording do not contain social security numbers if the inclusion of social security numbers is prohibited by law.

Therefore, recorders should be immune from suits relating to documents filed or recorded that include social security numbers, and any liability should be imposed on the document preparers.

Authority to Redact Post Effective Date

Model legislation may grant recorders the authority to redact social security numbers from documents that are recorded after the effective date of that legislation. This authority should not affect the integrity of the original recorded document. This can be accomplished by masking the information available to the general public, for example, on the Internet, using

redaction software that allows disclosure of the unredacted image on certified documents used for official purposes, such as probate.

This provision provides an important ministerial function - that of providing certified copies of records from government offices. Certification of public documents requires recorders and clerks to provide an exact copy of a recorded document. Recorders need to be explicitly empowered to redact the social security number after the effective date of the legislation, without compromising the integrity of future certified copies.

Voluntary Redaction by Public Prior to Delivery for Recording

Model legislation may grant members of the general public the opportunity to remove social security numbers and other private identifying information prior to the filing of their documents, such as the aforementioned Texas Property Code Section 11.008. This provision removes discretionary issues from the government official and provides members of the general public with a self-help remedy if they are concerned about the privacy of their personally identifiable information. If an individual removes a social security number or other personally identifiable information from the document before it is recorded, the recorder will be unable “undo” the redaction.

Recorders Not to Redact Information from Documents to be Recorded

Model legislation may provide that recorders **not** have the responsibility of redacting social security numbers or other personally identifiable information from documents prior to recording. Recorders would continue to record whatever they receive.

This provision continues the important ministerial, non-discretionary function - that of creating a public record of documents exactly as they were presented to the government offices.

Certification of public documents then complies with the recorders' and clerks' responsibility to provide an exact copy of the document as it was when recorded.

CONCLUSION

This White Paper has presented a multitude of issues faced by the land records industry and offered recommendations for what are considered either "best practices" or model legislation considerations as technology and privacy concerns evolve. In response to comments received from PRIA members and other commentators, the PRIA Records Access Advisory Policy Committee's Privacy Access Work Group is now moving forward to draft model legislation following the recommendations set forth within this White Paper.

Practical and informed policy making is a must to further solidify the integrity of our public records system and to achieve a meaningful balance between the public's concern about privacy and businesses' legitimate use of data. Enlightened policymakers have an opportunity to resolve these issues in a way that empowers consumers, enables business, and enhances our nation's economy.

APPENDIX I

Statement of Mark Ladd, Racine County Register of Deeds and Public Sector Co-Chair,
Privacy/Access Workgroup, Property Records Industry Association

Testimony Before the Subcommittee on Social Security
of the House Committee on Ways and Means

June 15, 2004

Good morning Mr. Chairman and members of the Committee:

My name is Mark Ladd. I am the Register of Deeds for Racine County, WI, and I am the Public Sector Co-Chair of the Property Records Industry Association (PRIA) Privacy/Access workgroup. I appreciate the opportunity to speak to you today regarding personal information and privacy issues as it relates to the land records industry.

The collateralization of real property is a fundamental part of our economy. Leveraging real property is possible because of the public availability of information regarding a specific parcel. Our nation's private land ownership is based on necessary access to publicly recorded real property information.

On the other hand, citizens are concerned that personal information is sometimes contained in real property records and may be used for criminal intent, such as identity theft. An example of sensitive information with little legal purpose, yet quite useful to identity thieves, is a Social Security number. Social Security numbers can appear in mortgage documents, tax liens, or even a divorce decree that conveys real property.

Privacy interests and the interest for disclosure of land records information often appear at odds with each other. The PRIA is convinced that a workable balance can, and in fact, must be reached on this issue. That balance should protect personal privacy without impeding commerce or overburdening land records offices.

PRIA hosted a roundtable forum on February 26, 2003 to discuss this issue. The 25 roundtable participants covered a broad range of representatives including representatives of the federal government (IRS and GAO), state and federal court systems, Land Records Officials, national associations in the real estate industry, as well as two influential organizations dedicated to consumer privacy issues.

At the conclusion of this meeting the PRIA established a Privacy/Access listserv as a forum to foster additional discussion on the topic.

The list serve discussion was followed by two days of facilitated educational discussions during our 2004 Winter Conference. During these discussions PRIA members reviewed the historical

foundations of American public records and then addressed the policy issue by debating several suggestions for model legislation.

It is with this background in mind that we offer the following comments relating to HR 2971.

Section 101 of the proposal contains a prohibition of the “display to the general public” of a Social Security number (Page 3, Lines 18 &19). “Display” is later clarified as “to intentionally place such number in a viewable manner on an Internet site.”

The Internet has become an important tool for many land records custodians to publish records. More and more counties are developing Internet based sites designed so that citizens can conduct business with government when it is convenient for the citizen and these sites can include data as well as images of documents.

The PRIA discussions reveal that few occurrences of the Social Security number in land records are required by any government agency with the exception of the IRS and state taxing authorities. The Social Security number is normally included by the document preparer for the benefit of their business practices or that of a business partner. While the problems associated with this practice may seem obvious to us, this is a standard practice with a number of financial institutions. Land records officials have no statutory authority under current law to refuse to record such documents.

In the bill’s current form, this provision would prevent land records custodians from posting currently recorded land records on the Internet, thus removing an important tool from our use. Even with this provision, SSN’s can still be included in public documents, placing individuals’ privacy at risk.

As I stated, the Property Records Industry Association has had extensive discussions regarding this topic and I would now like to offer our suggestions as to elements that this type of legislation should encompass.

1. Legislation should be effective on a “day-forward” basis. It should not require redaction or expungement in records already filed or recorded.
2. Consider prohibiting the inclusion of Social Security numbers on documents that will become part of the public record. This should include providing land records officials the authority to reject a document for filing/recording that includes a Social Security number. Practically speaking however, rejection authority needs to be permissive rather than prescriptive. The sheer volume of documents and the number of pages involved will make prescriptive authority difficult to manage.
3. Next we suggest that if a document recorded after the effective date of the legislation contains a Social Security number, the land records official should have the authority to redact the Social Security number from the document.

This is an important provision for an important ministerial function - that of providing certified copies of records in our offices. Our certification statement requires that we provide an exact copy of a recorded document. We need to be explicitly empowered to redact the Social Security number without compromising the integrity of future certified copies we issue.

4. The PRIA acknowledges the nearly impossible task faced by land records officials in attempting to keep Social Security numbers out of the public record and it believes this responsibility is more properly placed on document preparers and individual consumers. Accordingly, PRIA believes that, for any law prohibiting a Social Security number in land records, land records officials should be immune from suit relating to documents filed/recorded that include Social Security numbers.

While land records officials will assist when and where they can, the scope of the task of checking every page of every document for Social Security numbers is simply beyond their ability to perform. The time to prevent Social Security numbers from becoming part of the public record is when the document is created -- before the parties execute them, not when they are presented for recording.

Thank you for giving the PRIA the opportunity to address this important public policy issue. Our discussions and policy debates instruct us that the time to address this problem is during the drafting of the documents. We believe that our recommendations can achieve the goal of protecting Social Security numbers in regards to the public record without jeopardizing the flow of commerce or placing an unbearable burden on the shoulders of local government.

APPENDIX II

The Redaction Process

County governments are required by law to make official records available to the public. However, they also have the responsibility to protect the citizens' records from access by those who would use the information for criminal purposes. The redaction of sensitive information from public records is a method by which the data is "masked," or "blocked out," so that it is not visible on an electronic document or on a paper document, if the electronic document is later printed.

In the redaction process, software is used to search through documents for sensitive information such as social security numbers, bank account numbers, credit and debit card numbers, or the home address of a law enforcement officer. The software is "taught" to look for number patterns and to identify those patterns as highly likely candidates for redaction. When the software finds this sensitive information, the software either automatically "masks" the information or prompts the end-user to confirm the software's findings. The "original" digitized images are saved into a specific directory in the computer system so that they can always be retrieved, with certain security permissions, while the copies that have been "masked" are put into a separate directory from which images are pulled for public view in the office of the recorder or over the Internet. It is important to note that the redaction process does not restrict access to the entire document; it only restricts the viewing of the sensitive information within the document.

In Florida, which has a redaction statute, it is estimated that three percent of public record pages, for the period 1970 through the present, have at least one number that needs

to be redacted.¹⁶ Therefore, for a set of 25 million individual pages approximately 750,000 pages could require redaction.

¹⁶ Information provided by Carol Foglesong, Assistant Comptroller, Orange County, Florida.