CSPRA

COALITION FOR SENSIBLE PUBLIC RECORDS ACCESS

Personal Identifiers and Public Records

The Coalition for Sensible Public Records Access (CSPRA) is a non-profit organization dedicated to promoting the principle of open public records access to ensure individuals, the press, advocates, and businesses the continued freedom to collect and use the information made available in the public record for personal, commercial, and societal benefit. It is CSPRA's belief that the records of how our society governs itself at all levels and manner of government ought to be open and accessible to all.

Introduction

One of the hottest areas of contention in access policies concerns the inclusion of personally identifiable information in government data. Privacy advocates tend to prefer total exclusion of such information, but many critical business and civic functions depend upon access to such information. One of the legislative battlegrounds in the digital age, personal identifiers demand a more nuanced approach than the law currently allows. Without personal identifiers, public records about people become less accurate and obscure the truth about a person and their transactions, responsibilities, debts, crimes, civic activities, and duties. Identifiers such as date of birth and full address are public facts (with rare exceptions) in wide societal use. They should not be removed from public access, as they are critical to accurate identification and correlating data. They are widely available from many sources. Excluding them from public records will not make them private facts but it will hurt the legitimate uses of the records.

Public records are a critical source of the truth. When open and accessible, they are heavily relied upon for advocacy, accountability, commerce, marketing, public safety, and newsgathering. They provide a source for the truth about the behavior of our residents and licensed professionals, the ownership of property and corporations, the activities that influence the political processes, and the whereabouts of people. In short, they mimic what people living in smaller towns and communities in free societies have known and relied upon for centuries to thrive. Public records reflect what we have always known as a community, but only recently have we taken to electronically recording and filing such records so one could find and read them easily. The public truth became the public record and when we outgrew towns where everyone knew this oral truth, we fell back upon the public record to meet our need for reliable and true information.

Open public records are also a powerful equalizing force. When there is no public source, information and truth can still be obtained for a price that is not affordable to all. Many of our entrepreneurs, small businesses, ordinary people, political candidates, and community activists are direct and indirect beneficiaries of open records. With direct access to open records and indirect access through the products and services that non-profit and for-profit entities provide, they can compete with those of greater means. From James Madison to Thomas Friedman, the leveling effect of open and equal access to truthful information has been recognized as a bulwark of societal and economic equality. The truth cannot only make one free; truth grants equal opportunities to all.

Markets throughout history and especially of late have had their share of ignominious failures. These are due in large part to the absence of transparency and the greed that grows in shadows where truth's sunshine is shielded. Trading, capital, and other macro-markets depend heavily on true and complete information. Moreover, the consumer and service economy depend on population-wide demographic and individual information that will help target messages, goods, and services from willing legitimate sellers to willing buyers. These two forces—macro-markets and the consumer economy—run on truthful information. It is a critical resource in our modern economy equal to oil, lumber, computer chips, plastic, and steel. It is necessary for policy makers to finally achieve a common understanding of the importance of this fact and be mindful of it when addressing public records issues.

The Threats to Turn off the Truth

Identity Theft and Crime

There are growing and pervasive efforts to restrict the flow of public information.
A large share of the reason for such restrictions stems from the fear that public records in general and personal identifiers in particular, are a cause of identity theft and that closing public records will slow down or stop this crime. This has become the trump card of secrecy. Merely whisper the "identity theft" and public records slam shut regardless of the validity of the claim or the impact of hiding and redacting the truth.

Table 1

Overall Rank 2009	Overall Rank 2008	Item	Percentage 2009	Percentage 2008	Range of Prices
1	1	Credit card information	19%	32%	$0.85–$30
2	2	Bank account credentials	19%	19%	$15–$850
3	3	Email accounts	7%	5%	$1–$20
4	4	Email addresses	7%	5%	$1.70/MB–$15/MB
5	9	Shell scripts	6%	3%	$2–$5
6	6	Full identities	5%	4%	$0.70–$20
7	13	Credit card dumps	5%	2%	$4–$150
8	7	Mailers	4%	3%	$4–$10
9	8	Cash-out services	4%	3%	$0–$600 plus 50%–60%
10	12	Website administration credentials	4%	3%	$2–$30

Table 5. Goods and services advertised on underground economy servers
Source: Symantec

One would think that any claim that leads us to stifle the truth would be supported by overwhelming evidence. If we believe in a rational democracy and the truth itself, then the least we can do is ask for the evidence before we react. We have asked, we have searched, and the best we can find are anecdotes and assumptions, but no actual evidence to support the claim that public records cause identity theft to any

substantial degree or that their redaction will prevent it. What we have found instead is evidence to the contrary. We have found evidence that the majority of crimes identified as identity theft are actually credit card fraud. This has nothing to do with the public record since credit card numbers are not and should not be public. Except where credit card numbers are stolen from the government, credit card fraud has nothing to do with government records.

We have also found evidence that the criminals have changed their methods. Studies have shown that the theft of money and goods has moved from the small-scale theft and use of identity data, to wholesale theft of security keys and sophisticated cyber and phishing attacks (see Table 1 above from Symantec showing what is being purchased on the black market to enable theft and fraud). We have found evidence that the data in the public record that is targeted for closure and redaction is routinely available from other legal and black market sources. Finally, we have found evidence that open public records are often used to prevent and prosecute identity crimes, help prove the innocence of the victims of identity crimes, and help repair the damage caused by identity crimes. We have summarized some recent studies supporting this analysis in Figure 1.

Figure 1: Summary of Recent Studies (see Endnotes for Citations)

1. Of the $54 billion in identity theft and fraud, $22 billion is credit card fraud, $11 billion is existing account fraud, and $21 billion is new account fraud (Javelin, p. 10)
2. Public records are not a significant or easily used source of data leading to identity theft and fraud (Combs, pp. 2-5)
3. Un-validated, weak single factor authentication (usually something we know like a number or fact that is widely available or easily acquired) and a highly-evolved and unchecked cybercrime industry are the primary causes of identity theft, fraud, and crime, not personal data availability and access in public records (Combs, pp. 4-7)
4. Monitoring, Red Flags rules, and better cyber security work to reduce risk and loss from fraud (Javelin, pp. 9, 14), while closing public records does not (Combs, pp. 7-10)
5. 70 to 150 million or more personal computers can be controlled by a stranger (Trend Micro and Symantec)
6. Thieves do not need to do all the work to steal an identity when they can steal credit card numbers, passwords, and direct access to existing accounts and hence, these are the most popular tools of theft (Symantec p. 15)
7. Most of the personal data that government is trying to redact from the public record is in such wide use, has long been publicly available, is stored in countless and better organized non-governmental systems, and must be used so often, that it cannot be made secret no matter how much government tries to do so (Combs, pp 7-11)

We would also expect that anyone who wants to remove or block the truth from the public record would meet the burden of showing that the benefits outweigh the costs. Not only has this basic burden not been carried, it

has not even been hefted. The many redactions and record closings cost government an enormous amount in money, time, personnel, software, and lost opportunities. The cost to society and those individual and business users is a multiple of the government costs. Often the costs of solutions are passed on in the form of higher fees and taxes. Moreover the impact on commerce, newsgathering, democracy, entrepreneurs, financial markets, and consumers remains uncounted and unappreciated. Weighed against this staggering cost, there are no documented, quantifiable, provable benefits from closing and redacting public records. While we think it unrelated, it is worth noting that since redactions to prevent identity theft have begun, identity theft has *grown* to a record level. It is the duty of policy makers and jurists to fairly weigh the policy and legal options. In that weighing, there is but one possible conclusion: The scales remain precipitously tipped toward openness and truth, as nothing has been placed on other side of the scale of any substantial weight.

We have consistently advocated improved identity and information security and monitoring, more crime fighting personnel and resources, and increased international cooperation in tracking down and punishing cyber and identity criminals. When used, these measures have yielded results. However, they are not the weapons of choice our lawmakers, judges, and administrators are choosing first or in sufficient measure. If we are serious about stopping these crimes and protecting privacy, this must change and we must stop pretending that redacting the truth in public records is an effective or adequate countermeasure. Our suggested countermeasures are summarized in Figure 2 below. If doubts remain, please consider this question: If no personally identifiable information were left in any public record, would identity theft stop or even shrink? There is only one rational answer and that is "no."

Will the True Me Please Stand Up

Many proposals seek to eliminate unique identifiers such as social security number and personally identifiable data such as name and address from public records entirely or just from public records made available to the public. These proposals often, intentionally or not, apply even when there are legitimate and important public or private needs to uniquely identify a person. Since there is no common government system to do this, the public and private sectors have improvised one. Unique or distinct data such as date of birth, SSN, driver's license number, address, and so on is used in conjunction with name to positively identify a person. This is necessary because name alone cannot positively identify a person and properly connect events and behavior to the right person and their property. Doing so is the heart of responsibility in America today. Such affirmative identification was a formality when most of us lived in rural areas and everyone knew everybody else who resided there. Now, our reputations, credit, benefits, safety, and much more depend on the accurate identification of millions of Americans who are not our friends and neighbors.

The truth of massive populations who share many common names is that there is no way to preserve the integrity of the facts and the truth about a person without the other data elements. Because positive identification is so essential, we have allowed the use of these data elements to grow and become ingrained in numerous systems. It is these systems on which we rely for most public and private processes. Even if there was consensus to

change the broad use of these other data elements as unique identifiers, the needs we have, as civil and commercial society, to uniquely identify a person will not change. Some kind of system is needed and any new system would need to relate these existing data elements to names to maintain continuity of information for several generations. The question is not whether we should have unique identifiers, but how we manage them and use them. They cannot be eliminated from held or disseminated public records without harming the many legitimate uses of the data to determine with some certainty, who a person is and what records apply to them.

***Figure 2*—More Effective Countermeasures Against Identity Theft and Fraud**

Encourage and help everyone to:

1. Strengthen—use combinations of hard to fake authentication factors that represent something you know, own, and are
2. Monitor—use do-it-yourself or pay services to monitor credit reports and the use of personal information
3. Prevent—use free and fee-based credit alert and freeze services as well as transaction type and size limits on accounts
4. Secure—increase cyber security awareness and ability with training and up-to-date security tools and patches
5. Encrypt—make lost and stolen sensitive data unreadable with strong encryption
6. Reform—use and expand the Federal Trade Commission's Red Flags rule on opening, using, and altering financial accounts to cover all important accounts, transactions, and benefits
7. Enforce—hire and train more cyber cops

A final irony is that often legislation and rules seek to prevent transfer of unique identifiers to commercial entities to which we already entrust our unique identifiers. Financial institutions, credit bureaus, information brokers, insurance companies, lawyers, and so on already have our personal information such as social security number by necessity and, at times, by law. Not giving these commercial entities the personal identifiers in the public record to legitimately and accurately link events and behavior to the right person and their property protects no one but the imposters, harms the innocent, and hides the truth about the one true person that is the subject of that record.

Let It Flow: The Abundant Benefits Flowing from Public Records

The use of public records by the press and public for selecting and electing public officials and the oversight of government is well understood. Government that lives in the sunshine is closest to its people and to its purpose. But what is less appreciated and understood are the myriad of other uses of public records. Like any good system, this is mostly invisible and unnoticed by those whom it serves. Unfortunately, this means these uses of the truth can be taken for granted or stepped on without knowing the harm being done. We would all do well to better know that on which we so greatly depend, especially if the "we" are

those who make the laws and rules that affect public records and their use. Consider the following top activities that nourish our lives and our prosperity and that depend on accessible, complete, accurate, personally identifiable, and truthful public records:

1. **Life Events**
Many critical and routinely valuable events in our lives depend on the truth of public records. A reliable system of recording property owners and for assessing the credit worthiness of buyers and sellers means we can securely and economically buy and own a home, a vehicle, investments, and consumer goods of all kinds. The truth about those places and people who care for our youngest, oldest, infirm, and most needy helps us make the right choices and better protect those we love. Love itself is enabled by the truth in public records in that it helps us find a partner who truthfully represents themselves and their marital status. When our good behavior is reflected in an accessible and true public record, we are rewarded with work and life opportunities fitting out skills and character. Even the everyday life events depend on the truth—for instance, when we check to see how well a restaurant complies with the health code.

2. **Support for Legitimate Locator Services**
Whether we are seeking to recover a debt, to fairly administer justice and law enforcement, enforce a law, collect child support, find witnesses and bail jumpers, check out business's legitimacy and quality, discover unlawful or unethical dealings, or just find a long-lost ancestor, we often use public records to find who and what we need to know.

3. **Background screening for personal and workplace safety, security, and to protect vulnerable populations**
William Shakespeare said, "Love all, trust a few." In a world fast approaching seven billion souls and millions of businesses, how can we know whom to trust? Who has been convicted of serious crimes? Who is a sex offender? Who is a good credit risk or a safe driver or successfully employed? Given even the most obsessively long-lived extroverted individual could only briefly meet a few hundred thousand people in a lifetime, what happens when we need to trust a person we do not know? This is the essence of why background screening has been a growing, well-used, and well-liked process and business. We live in a global village without any of the communal and shorthand knowledge of the traditional village that helped us make rational risk-benefit decisions. The public, "unspinnable" record of a person's and a company's history is a rare and precious commodity that stands in for the knowledge of the village. The background check, substituting in the Internet era for what talking to one's neighbors used to accomplish, allows citizens of our connected world to make these risk-benefit decisions.

4. **Public safety and criminal activity detection, response, mitigation, and intervention**
Public records and the value-added services on which they are based are key investigative tools for government agencies, law enforcements, and security firms. The intelligent use of such records can prevent and detect fraud related to credit cards,

health benefits, insurance, and mortgages. Public records are often used to do identity verification of both individuals and businesses to prevent ID theft and fraud and help a victim recover their reputation after the crime. In addition to crime fighting, public records are key in product and vehicle notifications and recalls. They are also used to provide car history keeping sellers honest and letting buyers know of potential safety hazards from damaged cars.

5. Economic growth, fairness and job creation

It is often said that we live in an information economy. The natural resource on which that economy depends is information and public records are a critical source. Public and private data is used in combination to equalize access to business opportunities, provide convenient and personalized customer service, increase markets and market efficiency, and contribute substantially to economic growth. It is so ubiquitous, it is easy to forget that good information leads to target marketing and communications that help businesses get started or grow. We have achieved a degree of democratization of opportunity through equal and reasonably priced access to public information that strengthens the vitality of our entrepreneurial and small business sectors. It should not take difficult economic times to appreciate that the free flow of information is a job creation engine for our economy.

6. Helping residents exercise their right to know by indexing and adding value and services to public records

Many public records systems are by themselves sufficient to meet a particular need. Yet, these systems were never intended to meet all needs. Government sometimes struggles to keep up with new technology. Non-profits, citizens, commercial enterprises, academic institutions, and press entities among others fill in the gaps and expand the utility and accessibility of public records. Aside from being a valuable activity in its own right, these creative value added public records systems are great enablers of many other productive and useful endeavors. For example, public mapping and satellite systems contributed to what is now a well-known and appreciated success story known as GPS and personal navigation systems. There are countless others that enrich our lives and improve our productivity.

Conclusion

On the classic TV show Dragnet, the starring character Joe Friday was famous for saying, "All we want are the facts, ma'am." That, in a nutshell, is what we want from our government. This paper has implored that we all work to preserve our system of open government to give to us all the true facts that are in the public record. We have had to implore because the threats to the truth are many and are often without a solid foundation in facts or democratic principles. We have shown that there are better countermeasures to information misuse and fraud than hiding the truth. We have shown that the benefits of the truth are great and the risks from hiding it are too high to justify.

Endnotes

1. Social Security Numbers, Public Records, and Identity Theft, Combs, Daniel, 2008, available at http://www.cspra.org, under Recommended Reading
2. 2010 Identity Fraud Survey Report, Javelin Strategy and Research, February 2010, at http://www.javelinstrategy.com
3. Symantec Global Internet Security Threat Report, Symantec Corporation, Marc Fossi Executive Editor, Volume XV, Published April 2010 http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xv_04-2010.en-us.pdf
4. Federal Trade Commission Red Flags Rule, see generally http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus23.shtm. The Red Flags Rule was promulgated in 2007 pursuant to Section 114 of the Fair and Accurate Credit Transaction Act of 2003 (FACT Act), Pub. L. 108-159, amending the Fair Credit Reporting Act (FCRA), 15 U.S.C. § 1681m(e). The Red Flags Rule is published at 16 C.F.R. § 681.2.