CSPRA

THE COALITION FOR SENSIBLE PUBLIC RECORDS ACCESS

September 5, 2007

Via Electronic Filing

Mr. Donald S. Clark, Secretary
Federal Trade Commission
Room H-135 (Annex K)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Re: SSNs In The Private Sector—Comment, Project No. P075414

Dear Secretary Clark:

The Coalition for Sensible Public Records Access (CSPRA) is a non-profit organization dedicated to promoting the principle of open public record access to ensure consumers and businesses the continued freedom to collect and use for personal and commercial benefit the information made available in the public record. We look forward to continued leadership by the FTC on information policy and thank you for the opportunity to provide input into the SSN issues. We offer the following information and comments on four of the five listed topic areas.

Current Private Sector Collection and Uses of the SSN

There are a large number of public and 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. The SSN is at the heart of this improvised scheme. There is no way to preserve the integrity of the facts and the truth about a person without SSN since we have allowed its use 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 SSN as a unique identifier, the needs we have as civil and commercial society to uniquely identify a person will not change. Some kind of system will be needed and any new system would need to relate to the SSN 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.

The most obvious yet important fact in reviewing private sector use is that names are not unique and numbers can be. Without pairing a name with a secondary fact such as SSN that is unique, many false positive and false negative conclusions and outcomes result. People will be improperly given positions of trust over property and vulnerable people

and receive benefits for which they are not qualified. Similarly, people will be unfairly denied rights, benefits, and privileges which they are due or the process of exercising and using them will be difficult.

We are especially concerned as to how the many proposals to limit or eliminate use of the SSN will affect the accuracy and reliability of public records. Besides obvious public uses by government employees (especially law enforcement), SSN linked records are used extensively by the private sector in areas such as background screening, identity verification, drug screening, debt collection, mortgages and other credit, e-commerce, risk management, research, citizen oversight of institutions, and similar uses that require unique identification. Many of these private sector services are in turn consumed by public sector entities for governmental purposes such as fraud detection, delinquent child support payment, licensing, sex offender tracking, and so on. This dynamic flow of information will be crippled from restrictions on the use of SSN. The primary result will be that we will be unable to effectively link people to behavior so that the proper positive or negative consequences result. This is a bedrock reason why records are public in the first place. There is no alternative system and any migration to such an alternative would take a substantial amount of time and money. Without a clear path forward, making changes in information infrastructure on which we depend is unwise.

In sum, major limitations in the use of SSN as a unique identifier in public records will have many known negative consequences, are likely to have substantial unintended consequences, have not been shown to have beneficial effects worth the cost or disruption in the flow and value of public information, and will create a redacted version of the truth that is at odds with the purposes of public records.

The Role of the SSN as an Authenticator

There are two types of uses for SSN as an authenticator: analytical and transactional. An analytical use is one that associates other data elements with the SSN to gather insights and form the basis for decisions and conclusions about a person. A transactional use is when a SSN is used as one of the facts presented by a person to gain rights, benefits, and privileges in the name of the person associated with an SSN number. Most of the benign and benevolent uses of SSN flow from analytical uses. Most of the detrimental uses of SSN stem from use of it in single factor authentication processes. A single factor process uses only data elements that are things which a person knows. Moreover, the things "that we know" that are often used for authentication are in wide circulation and very hard to keep secure. The other two factors of authentication—something one has (a card or other token) and something one is (evidenced by some biometric measure)—are not used often enough in the process of granting or denying rights, benefits, and privileges. With proper identity security systems, risks are mitigated (not eliminated) according to the risk involved in the transaction or activity. The more risk, the more factors of authentication that need to be used and the stronger they need to be. The lack of a three factor, risk adjusted authentication system is the root cause of the vast majority of concerns about personally identifiable information. While there are other legitimate concerns about privacy in analytical uses of SSN, the excessive reliance on SSN in transactional

authentication is the catalyst for most of the public policy activity today. The transactional use of SSN and lack of proper identity security systems is where we suggest policy makers focus their attention.

In sum, much of the concerns about SSN in public records stems from inadequate identity security systems that overly rely on single factor transactional authentication using facts that cannot be kept secure such as the SSN.

The Role of the SSN in Fraud Prevention

Public records are often used to thwart fraud. Many public and private systems link the SSN to other public facts to detect fraud in individual cases and as a pattern inside systems. It is this linking of data elements to a common identifier that allows these systems to detect anomalies and errors that point to fraud. Without reliable data that has a common unique identifier, more fraud results.

In sum, it may be counterintuitive to think that more information reduces theft by fraud, but most human endeavors rely on numerous and free flowing sources of information improve accuracy and find errors. Fraud detection is no different.

The Role of the SSN in Identity Theft

Many jurisdictions are grappling with identity theft, fraud, and misuse. The primary approach proposed in much of the legislation is to prevent misuse of identity by limiting the revelation of certain data. In most cases, and especially in the case of Social Security Numbers, this is a very ineffective prevention tool. Data, especially data in wide use and circulation, cannot be kept adequately secure. To the extent we keep depending on keeping a few numbers and letters secret to prevent the misuse of identity we will continue to fail and remain the most vulnerable identity theft target country in the world. There are too many ways to get this information and too many points of failure—human, physical, and software—for this data to be kept secret.

A much more effective approach is to adopt identity security policies and infrastructure that govern the granting of rights, benefits, and privileges. Identity security is the process by which a person presents themselves to another for the purpose of obtaining rights, benefits, and privileges due to that person. At the point of presentment, one to three factors of identity are presented. The three factors of identity are something one knows (a PIN, password, or a sufficiently obscure fact), something one owns (such as a token, card, cell phone, or other unique object) something one is (represented by some form of biometric such as a photo, fingerprint, iris print, voice print, etc.). These three factors can vary in strength. For example, a password can be simple or long and complex. The number of factors that are used and the strength of those factors vary with the risks involved in the transaction and the risk-avoidance preferences of the user. Identity security is the only proven method by which risks of misuse, false positives, and false negatives in the granting of rights, benefits, and privileges can be adequately mitigated

and often prevented. Security in depth with proper identity security is the only way to actually affect identity theft, fraud, and misuse.

In sum, while SSN and any personally identifiably information can play a role in identity theft, the information itself is not the cause of the problem. The root cause is our sole reliance on such facts to grant rights, benefits, and privileges.

Thank you for your consideration of our input.

Richard J. H. Varn
Executive Director
Coalition for Sensible Public Records Access
620 42nd St
Des Moines, IA 50312-2732
Email: rjmvarn@msn.com
Office: (515) 255-3650
Cell : (515) 229-8984
A non-profit organization dedicated to promoting the principle of open public record access to ensure governments, consumers, and businesses the continued freedom to collect and use for public, personal, and commercial benefit the information made available in the public record.