

September 5, 2007

Donald S. Clark
Secretary
Federal Trade Commission
Room H-135 (Annex K)
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: SSNs in the Private Sector—Comment Project No. P075414

Dear Mr. Clark:

Thank you for the opportunity to respond to the July 30, 2007, request of the Federal Trade Commission (FTC) for public input on private-sector uses of Social Security numbers (SSNs). I am a Distinguished Professor at the Indiana University School of Law-Bloomington, director of Indiana University's Center for Applied Cybersecurity Research, and a Senior Policy Advisor in the Center for Information Policy Leadership at Hunton & Williams (the Center).

These comments are submitted in my capacity as a Senior Policy Advisor in the Center. The Center was founded in 2001 to develop innovative, pragmatic approaches to privacy and information security issues from a business-process perspective while respecting the privacy interests of individuals. These comments have benefitted from the Center's extensive work on identity verification and authentication and the input of Center members, but they do not necessarily reflect the views of the Center or its members.

These comments will address the critical roles that SSNs play in aiding in the identification of individuals and helping to ensure that data about an individual is accurately associated with that individual, and the challenges to accomplishing these vital tasks. Rather than attempt to restrict the availability of SSNs, the government should focus its efforts on addressing three issues that threaten the use of SSNs for these important purposes:

1. The inappropriate use of the SSN as a default password or as a stand-alone evidence of identity;
2. The use of the SSN by criminals to impersonate others and commit fraud; and
3. The difficulty the government faces in ensuring that its system for issuing, maintaining, and canceling SSNs is efficient and accurate.

These comments conclude by recommending that the policy discussion should focus not on the SSN, but on how best to meet the needs of identifying individuals, verifying identities, and accurately linking data to individuals.¹

¹ These comments address SSNs in the private sector in connection with commerce and consumer transactions rather than the employer-employee relationship. Legal requirements concerning the use of SSNs in the employment context raise important issues that are beyond the scope of these comments.

The Role of SSNs as Unique Identifiers

As FTC Chair Deborah Platt Majoras testified before the Senate Commerce Committee in 2005, “Social Security numbers today are a vital instrument of interstate commerce. With 300 million American consumers, many of whom share the same name, the unique 9-digit Social Security number is a key identification tool for business.”² Indeed, SSNs currently fill three critical roles in the private sector as identifiers of individuals. The first is aiding in the identification of individuals—helping us to differentiate among individuals with the same or similar names. The second role is assisting in verifying that the person presenting himself or herself—to apply for instant credit, seek a government benefit, or board an aircraft—is who he or she claims to be. The third is helping to ensure that data about an individual is associated with that individual and no one else.

The first role—the identification function—is clear and critical. Too many people share the same or similar names—there are more than 60,000 John Smiths and 43,000 Robert Joneses in the United States alone³—and, as discussed in greater detail below, addresses change too frequently and are subject to too many variations for either to serve as reliable identifiers. As a result, a distinctive number is required.

The second role—identity verification—is often misunderstood and, on occasion, still misapplied in practice. Obviously, the fact that an individual presents an SSN does not prove that he or she *is* the person that the SSN identifies. Rather, the SSN, when combined with other information, provides an efficient, reliable way of locating a credit report or other record containing information that can then be used to verify the identity of a person. So, for example, if I call a financial institution to perform a transaction or obtain account information, I may be asked for my SSN (and other information) to link me to the right account; information in that account can then be used to verify my identity. Or if I apply for instant credit at a retailer, the retailer may ask for my SSN as a way of locating a summary credit report about me. That credit report may list, among other things, my name, address, phone number, past addresses, and other identifying information. The retailer can then compare the information I have put on the credit application with the information contained in the credit report to determine if I am who I claim to be.

Knowing the SSN alone does not and should not be used to establish identity; it is merely an effective way of locating reliable information about an individual that then can be used to verify his or her identity. SSNs do not have check digits, they are often mistyped in records, they have been issued to more than one individual, and fraudsters intentionally link SSNs to fictional

² *Data Breaches and Identity Theft*, Hearing of the Committee on Commerce, Science, and Transportation, U.S. Senate, June 16, 2005 (prepared statement of the Federal Trade Commission).

³ *Enhancing Social Security Number Privacy*, Hearing of the Social Security Subcommittee of the House Ways and Means Committee, June 15, 2004 (statement of Brian McGuinness).

people. The SSN is not proof of anything related to identity; it is merely a link to data that can be used to verify identity.

SSNs also play an essential third role: helping to ensure that data are linked to the right individuals. SSNs help to ensure the accuracy and completeness of records. As a result, individuals can be treated fairly and subsequent users of the data have confidence in the data. When an individual applies for instant credit or an auto loan or a mortgage the lender wants to know that it is seeing an accurate and complete picture of that individual's creditworthiness and that there will be reliable, affordable ways of determining if the individual declare bankruptcy or overextends himself or herself on credit in the future. SSNs facilitate the correct linking or association of data in the databases that do this. This is critical to ensuring that the underlying data store is sufficiently accurate and reliable to support not only credit and other important decisions, but also the identity verification function described above.

The Challenge of Accurately Linking Data and People

The challenge of associating the right data with the right people is greater than might first appear. Consumer and privacy groups have highlighted the magnitude of this challenge in their complaints about alleged inaccuracies in credit reports and public records. The heart of their charges is not that the data are wrong, but that they are linked to the wrong person. This challenge is exacerbated by many factors, including:

- The frequency of common names and the fact that names are not constant, thanks in part to 2.3 million marriages and 1.1 million divorces every year.⁴
- The variety of addresses available to many people (e.g., home, office, vacation home, Post Office box), the fact that several people may share the same address, and the speed with which addresses and telephone numbers change: according to the U.S. Postal Service, approximately 17 percent of the U.S. population—about 43 million Americans—changes addresses every year; 2.6 million businesses file change-of-address forms every year.⁵
- The inconsistencies with which we record names (e.g., J. Smith, J.Q. Smith, John Q. Smith) and addresses (e.g., “123 Main,” “123 Main Street,” “123 Main St.,” “123 S. Main Street,” “123 Main Street, Apt. B”).
- The spread of first telephone and then Internet technologies, the increased mobility of the population, and the development of truly national competition mean that fewer transactions are conducted face-to-face, much less with people we know.

⁴ National Center for Health Statistics, *National Vital Statistics Reports*, vol. 51, no. 8, May 19, 2003, at 1, table A.

⁵ United States Postal Service Department of Public Affairs and Communications, *Latest Facts Update*, June 24, 2002.

As a result of these and other factors, the need for a unique, ubiquitous, national, constant, and authoritative identifier has become inescapable. Many activities in which we engage in both public and private sectors are impossible or impractical without it. That is why the SSN has evolved to fill this role: modern government and business activities required it to identify individuals and ensure that information about one individual is not erroneously attributed to another individual.

Ironically, the need for unique identifiers is so great that data systems which for legal or other reasons do not rely on SSN, have consistently had to create other unique identifiers. Where those data systems interact with each other or with systems that require SSNs (e.g., payroll, tax, etc.), they must employ translation tables to link one unique identifier with another. This introduces inefficiencies and greater risk of errors, as well as requires creating and maintaining new datasets of potentially sensitive information.

SSN Recommendations

There are, of course, problems with SSNs in our society today. Three are especially acute.

First, some institutions use SSNs inappropriately as a default password or as stand-alone evidence of identity. This is akin to using street address or telephone number as a password or proof of identity. It is inappropriate, and policymakers would do well to discourage such uses through education, regulatory oversight, and, if necessary and after an appropriate opportunity for updating or replacing legacy systems, prohibition, enforcement, and prosecution. Similarly, the government should evaluate whether its increased reliance on the SSN in employment and other settings is appropriate.

Second, criminals seek to use SSNs to impersonate others and commit frauds. This exploitation in part seeks to take advantage of the inappropriate role given SSNs by some institutions. So, for example, a business that sets default consumer online account passwords to SSN invites the fraudulent use of SSNs by criminals seeking illegal access to those accounts. Eliminating those inappropriate uses will curtail those criminals' efforts to exploit the SSN.

But other criminals seek to use SSNs even in settings where they are being appropriately used. This almost always requires combining the SSN with other data. The criminal then fraudulently presents the SSN as his or her own, for example, when applying for credit, and attempts to supply the other data (e.g., name, address, account information) from other sources that the creditor will match with the data linked to the SSN in an effort to verify identity. This is a real and growing risk, but it is not best addressed by restricting the availability or use of SSNs. In fact, restricting access to SSNs may be counterproductive, since fraud tools to detect the patterns associated with fraudulent use of SSNs often require access to SSNs.

Moreover, since other unique identifiers will just take their place, restricting access to SSNs will only have the effect of pushing the attempted fraud from one identifier to another.

Rather, more effective responses are to create incentives for the more accurate matching of less readily available data, encourage the use of SSN-related data matching in connection with other identification tools, enhance penalties for the fraudulent use of SSNs and the creation of fabricated SSNs, vigorously enforce SSN fraud laws, and intensify research into other means for verifying identity.

It is striking both how obvious the need to make SSNs harder to exploit is and how little policymakers have focused on it. The Strategic Plan issued in April by the President's Identity Theft Task Force, for example, identified "making it harder to misuse consumer data" as one of its four strategies for combating identity theft, but then offered only two specific recommendations for implementing this strategy: "hold workshops on authentication" and "develop comprehensive record on private sector use of SSNs."⁶ I urge you not to fall into this same trap; making SSNs harder to misuse will not be simple, but it is an important goal and worthy of your sustained attention.

The third problem with SSNs today, especially given their importance in a wide range of settings, is ensuring that every individual has a unique SSN, that they are linked to the correct person from the start, that the government does not issue duplicate SSNs, and that the registry of deceased person's SSNs is kept up-to-date. In short, it is essential that the Social Security Administration makes certain that the system of issuing, maintaining, and canceling SSNs is efficient and accurate.

In summary, rather than attempt to restrict the availability or appropriate use of SSNs, policymakers should instead focus on how to restrict their inappropriate use. In fact, given the importance of accuracy in data matching and in linking people to data, we should be encouraging, not diminishing, the appropriate use of SSNs. The alternative is less accuracy, less efficiency, and greater risk as different users or groups of users create their own unique identifiers and then have to create translation tables to equate them.

The recent trend among policymakers to encourage the treatment of SSNs as secret information creates the misimpression among individuals and institutions that they can be used alone for identity verification, as if knowing a SSN somehow proved that you were that individual. This is unfortunate and could easily be avoided by treating SSNs as the public information they have historically been. This would focus attention on their appropriate use, and make clear, once and for all, that they are not appropriate to use as passwords or proof of identity themselves.

A Misfocused Policy Debate

The reality of the essential roles that the SSN plays as an identifier and the challenges the SSN is essential to overcoming suggest that the current debate over SSNs is misfocused. Banning private-sector uses of the SSN would solve no problems. In fact it would exacerbate

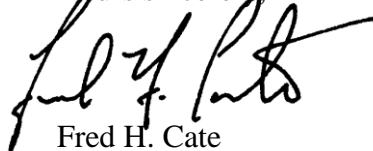
⁶ The President's Identity Theft Task Force, *Combating Identity Theft: A Strategic Plan* 42 (2007).

current problems related to fraud and authentication. SSNs are not the issue, rather, it is the need to distinguish among individuals, verify identity, and accurately link data that should be the focus of our concern. If Congress eliminated the private-sector use of SSNs tomorrow, another unique identifier would of necessity be created. We could call it something different than SSN, but it would have to serve the same purposes and it would present the same issues. Policymakers should therefore be concerned with those underlying issues.

This may not always be the case: new data-matching technologies and algorithms are already enhancing the ability of some sophisticated organizations to match data without SSNs and research is continuing into tools for verifying identity that do not involve data matching. But for the present, SSNs are widely relied on as part of the process for verifying identity and ensuring that information is associated with the correct person. Policymakers and the public have a significant interest in ensuring that both of these tasks are carried out accurately, efficiently, and reliably. Ensuring that—whatever the means—is the critical issue on which our attention should be most focused.

The Center for Information Policy Leadership and I stand ready to assist in fostering an informed and thoughtful discussion on these issues. Again, thank you for the opportunity to submit these comments.

Yours sincerely,

A handwritten signature in black ink, appearing to read "Fred H. Cate", written in a cursive style.

Fred H. Cate
Senior Policy Advisor