November 30, -0001

The Congressional Research Service is a $100 million a year think tank that researches and writes informative and non-partisan reports on topics suggested by members of Congress. The catch--and the reason you might not have read their work--is that CRS reports are only made easily available to members of Congress. Citizens can request these reports from lawmakers, but without a public index, they can't request something they don't know exists. The CRS Reports currently rank first on CDT's Most Wanted Government Documents. In an ongoing effort liberate these documents, CDT runs Open CRS, an online repository of public CRS Reports. To spotlight these reports, I will be writing "CRS Report of the Week" posts and feature a relevant report each week. These reports are informative in both that they serve as excellent primers to political issues and that they offer a degree of insight into what information is circulating around Congress. The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality #RL30318 October 2nd, 2008 It is well known that Social Security Numbers (SSNs) should not be used as authenticators. A new study demonstrating the ease with which SSNs can be predicted [http://blog.cdt.org/2009/07/06/study-proves-that-ssns-are-terrible-authenticators/] serves as further evidence to this fact. Simply put, SSNs weren't designed to be authenticators. The problem with SSNs is that they have become both the de facto national identifier and authenticator for private industry. This is analogous to using your name (an identifier) as your password (an authenticator). Identifiers are simply a reference to who you are and, thus, are often public. Authenticators, on the other hand, are used to prove identity, and should not be known publicly. These dual uses of SSNs as identifiers and authenticators has worried identity experts for some time because of this difference in security levels. The new research steps over those concerns and suggest that SSNs should never be used as authenticators not just because of the risk an individual's SSN might be disclosed, but because SSNs are predictable based upon publicly available information. Ultimately, it does not matter how vigilant one is in protecting his or her SSN. It can easily be discovered. This CRS report provides an overview of several laws regulating SSN use by the federal government. The two major statutes are the Privacy Act of 1974 and the Tax Reform Act of 1976. The Privacy Act discouraged government agencies' use of SSNs as identifiers by requiring that government services not be denied simply because an individual chooses not to disclose their SSN. However, agencies may require the collection of SSNs if a Federal statute requires it, or if the agency already had record systems based upon SSNs. The Tax Reform Act, two years later, only solidified the use of SSNs by requiring the use of SSNs on federal tax forms. SSN use as an identifier is entrenched the government, despite numerous examples of the widespread use and abuse this practice [http://www.gao.gov/highlights/d06586thigh.pdf]. Current law focuses primarily on SSN disclosure by the federal government in public records. However, given this research, disclosure does not seem to be the greatest concern if SSNs are predictable from public information. The main problem is the widespread use of SSNs as authenticators in the private sector for activities like credit approval or background checks. There are no federal laws that prevent private entities from requiring SSN disclosure, in which the SSN is likely used as an authenticator, as a condition to their providing goods and services. Given the entrenchment of SSNs as authenticators, it is unlikely that their use in the private sector will change any time soon.