The Social Security Number: The Wrong Tool for the Job

Subject Area General

EWS 2006

The Social Security Number: The Wrong Tool for the Job
Submitted by Captain BJ O'Loughlin
to
Maj GS Benson and LCDR BD Kincaid, CG 14
07 February, 2006

1. REPORT DATE **2006**	2. REPORT TYPE	3. DATES COVERED **00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE **The Social Security Number: The Wrong Tool for the Job**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **United States Marine Corps,Command and Staff College, Marine Corps University,2076 South Street, Marine Corps Combat Development Command,Quantico,VA,22134-5068**	8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**11**	

The Social Security Number (SSN) has weaved its way into the daily functioning of the military. It is used to identify Marines and their family members at nearly every level of the organization. However, the SSN has also become a powerful administrative tool with regard to an individual's personal identity. The Social Security Number has become too dangerous to use as an everyday administrative tool because of its universal acceptance, identity association, and status as "identifier of choice" for criminals. Rather than using Social Security Numbers for administrative purposes, the military should assign separate service numbers to its members.

Small Beginnings to Universal Acceptance

At first, SSNs were issued to help record the taxes paid by the holder into the Social Security System. The use of the SSN since its inception however, has changed significantly.

"the SSN's main purpose continues to be as an identifier for each worker's covered earnings; however, its uses have significantly expanded over time. By the early 1940's, it was realized that the SSN could be utilized by other agencies whenever personal identifiers or account numbers were needed."[1]

The SSN has infiltrated most of our society, "virtually all non-working children under age 15 now need or have the opportunity to apply for an SSN."[2] In 1967, the military used it to replace all service numbers.[3] So many agencies' accounting and recording systems eventually adopted the SSN as a means of identifying participants: an American (and foreigners working in America) could not function at virtually any age without one. The SSN has become a universal identifier of Americans, and is an important common denominator with regard to access of peoples' finances, health records, educational history, and civic activity information.

The Key to Your Identity…and theft

The SSN, plus a few other pieces of personal information become a person's identity. A Social Security Number and a combination of name, date of birth, telephone number, or in some cases mother's maiden name are all that is required to apply for credit, secure utilities, or tap into a person's health history, driving records, financial assets and buying preferences.[4] Once a few pieces of a person's identity are collected, the rest of a their information can be referenced fairly easily; "the Social Security Number is the figurative Rosetta Stone for unlocking financial, criminal, and medical information."[5]

Identity theft is one of the fastest growing forms of crime in the United States. "There is little doubt that identity theft

2

is growing in frequency and severity, exacting an enormous social and financial toll."[6] In 2001 over 86,000 complaints of identity theft were received by the Federal Trade Commission.[7] Last Year that number grew to 246,000.[8] In 1998, Tony Gwynn of the San Diego Padres was a victim of identity theft. A thief got a hold of his SSN, and a couple of other pieces of personal information.[9] In 2004, a Red Cross employee was caught after she allegedly used names and SSNs of blood donors to apply for credit cards, cash checks, and to collect bank loans.[10] Access to powerful information such as Social Security Numbers can lead to fraud and identity theft. Any organization which uses them could potentially put people at risk.

The military may be forced in the near future to reinstate service numbers anyway. Legislators have been exploring limiting the use of the SSN to its original purpose. If this limitation were to happen, then the military would no longer be permitted to use the SSN for identification, and therefore would be forced to find another way to identify members.[11] This proposed legislation may be a long-shot, but until something like it is approved, the military should attempt to mitigate the hazards of the SSN.

Too Prolific; Too Dangerous

For almost thirty-eight years, the Marine Corps has used SSNs as the chief means of identifying members at all levels of

command. From platoon leaders' notebooks to company rosters to Personnel Administration Centers, use of the SSN is an integral part of day-to-day Marine Corps life. The number is printed on manifests and rosters, health and dental treatment records, identity tags and identification cards. Leaders are taught to know their Marines' important information, including their SSNs. Any platoon sergeant can produce the Social Security Number for any of his or her Marines. Many people using this information on a regular basis increases the risk of identity theft for military members and their families.

Another danger is if a Marine is captured during combat operations against an enemy of the United States with his or her Common Access Card (CAC) and Identity Tags. Even before questioning the prisoner, the enemy has enough information to seriously injure this Marine and his or her family. They have enough information to attack this Marine's private records, family, and neighbors by accessing his or her identity and causing havoc. Since the rise of terrorist action against Americans, this kind of "identity theft" can lead to devastating effects on American families.

Current Measures in Place

Whenever information is handled by an organization, it may become vulnerable to theft. Professional thieves may use a variety of means to gather information from computer hacking to

4

"dumpster diving" for sloppily discarded documents.[12] Amateurs

may gather and improperly use information only when the

opportunity presents itself. For instance, a Marine lance

corporal accused of credit card theft stated that he would not

have considered theft at all had the credit card not been left

unattended. This type of "opportunity" can be avoided by

increasing security awareness and implementing sound theft

prevention measures from the institutional to the personal

level.

Marine Corps Order P5211.2B outlines the responsibility

inherent to every unit at every level of command. "Each system

manager will establish administrative, technical, and physical

safeguards to protect each system of records from unauthorized

or unintentional access, disclosure, modification, or

destruction."[13] Social Security Numbers are included in the

definition of records in this case. The order further states

that a responsible individual will be designated at "every

Marine Corps activity" to ensure the safeguarding of the

activity's system of records. The tenets of the above order are

not taken lightly, as indicated by its presence in the Automated

Inspection Readiness System (AIRS) Detailed Inspection

Checklist.[14] Administrative sections are thus tested on their

safeguarding of sensitive information such as SSNs during

Commanding General's Inspections (CGI) as well as Marine Corps

Administrative Analysis Team (MCAAT) inspections.

Some may believe that the reinstatement of service numbers

in unnecessary since the military already has measures in place

to protect this information. Marines are trustworthy, and

generally do the right thing with the information they handle,

including SSNs. The chance of this information getting into the

wrong hands however is higher if more people are required to

work with the information regularly. Considering the overall

importance of the SSN, its use at so many levels represents an

unnecessary risk to our Marines and their family members.

Replacing the Service Number with the SSN may have been a good

idea in 1967, but times have changed. The military must find a

way to properly administrate while mitigating the risks

associated with the SSN.

The Solution

Social Security Numbers are the right tool for identifying

service members, but they are the wrong tool for protecting

them. The solution is the return of the service number for

identification, thus reducing the risk of its misuse. One

course of action includes assigning a service number to all

Marines and associating their family members to that number in

the same fashion as the SSN. That number could be used for all

internal Marine Corps and Navy administrative functions. The

service number would be associated with the SSN only within organizations required to use it.

For example, a Personnel Administration Center submits two unit diary entries on a Marine using his or her service number. The first entry is the award of the Good Conduct Medal. The second entry starts his or her Basic Allowance for Housing (BAH.) The first entry uses only the Marine's service number to update the Marine Corps Total Force System. The second entry is initiated using the service number, but when the information reaches Defense Finance and Accounting Service (DFAS) the service number is associated by computer with the Marine's SSN for reporting purposes. The number of Marines required to handle the SSN are greatly reduced in this manner. The chance for misuse of the number is also reduced.

The SSN has grown into a powerful administrative tool and a crucial element of a person's identity. It is also used at all levels of command to identify Marines and family members. This reliance on the SSN as a service number puts Marines in jeopardy of identity theft or worse. The military needs to reinstate the Service Number as the primary means of identification in order to mitigate dangers of identity theft to service members. Although measures are in effect to safeguard the SSN from improper use, the routine manner in which this information is

used represents an unnecessary risk to service members and their families.

Transitioning to the service number would most likely be a massive and difficult endeavor. It would undoubtedly require close coordination between most federal organizations. While reinstating service numbers would require a serious commitment from the Department of Defense and most other federal agencies, it would be well worth the trouble.   Word Count 1559

---

[1] Wayne S. Long, "Social Security Numbers Issued: A 20-Year Review," Social Security Bulletin 56, no. 1 (1993), http://www.questia.com/PM.qst?a=o&d=5000191380.

[2] Long, "Social Security Numbers Issued."

[3] Long, "Social Security Numbers Issued."

[4] Sheila R. Cherry, "Getting to Know All about You," *Insight on the News*, February 7, 2000, 24, http://www.questia.com/PM.qst?a=o&d=5001153032.

[5] Stefan Linnhoff, and Jeff Langenderfer, "Identity Theft Legislation: The Fair and Accurate Credit Transactions Act of 2003 and the Road Not Taken," *Journal of Consumer Affairs* 38, no. 2 (2004), http://www.questia.com/PM.qst?a=o&d=5008649453.

[6] Linnhoff and Langenderfer, "Identity theft Legislation."

[7] Sheila R. Cherry, "Keep an Eye on Who Gets Your Number: The Social Security Number Has Become the National Identification Code-One Fraught with Security Loopholes and Serious Implications for Privacy Rights," *Insight on the News*, July 15, 2002, http://www.questia.com/PM.qst?a=o&d=5000793739.

[8] "Identity-Theft Case the Latest in a Series; Consumers' Vulnerability to Fraud Rises," *The Washington Times*, 22 February 2005, C07, http://www.questia.com/PM.qst?a=o&d=5008729700.

[9] Cherry, "Getting to Know All about You."

[10] "Identity-Theft Case"

[11] Linnhoff and Langenderfer, "Identity theft Legislation."

[12] Cherry, "Getting to Know All about You,"

[13] Marine Corps Order P5211.2B, "The Privacy Act of 1974," 8-3.

[14] "Automated Inspection Readiness System Detailed Checklist" 065, 19 January 2005

Bibliography

Automated Inspection Readiness Checklist 065,"Privacy Act,"
     January 19, 2005.

Brown, Monique R. "Protect Your Identity." *Black Enterprise*,
     January 2000, 117.
     http://www.questia.com/PM.qst?a=o&d=5001124240.

Cherry, Sheila R. "Al-Qaeda May Be Stealing Your ID: Stolen
     Credit Cards and Purloined Social Security Numbers, Fake
     Passports and Forged Documents-All Have Become Weapons of
     War for Terrorists." *Insight on the News*, August 26, 2002,
     18+. http://www.questia.com/PM.qst?a=o&d=5000817858.

Cherry, Sheila R. "Getting to Know All about You." *Insight on
     the News*, February 7, 2000, 24.
     http://www.questia.com/PM.qst?a=o&d=5001153032.

Cherry, Sheila R. "Keep an Eye on Who Gets Your Number: The
     Social Security Number Has Become the National
     Identification Code-One Fraught with Security Loopholes and
     Serious Implications for Privacy Rights." *Insight on the
     News*, July 15, 2002, 16+.
     http://www.questia.com/PM.qst?a=o&d=5000793739.

Cordesman, Anthony H., and Justin G. Cordesman. *Cyber-Threats,
     Information Warfare, and Critical Infrastructure Protection
     : Defending the U.S. Homeland /.* Westport, CT: Praeger,
     2002. http://www.questia.com/PM.qst?a=o&d=102120393.

Cronin, Michael A. "Fifty Years of Operations in the Social
     Security Administration." *Social Security Bulletin* 48, no.
     6 (1985): 14-26.
     http://www.questia.com/PM.qst?a=o&d=5001689110.

Gips, Michael A. "Victims Describe Identity Theft." *Security
     Management*, August 2000, 16.
     http://www.questia.com/PM.qst?a=o&d=5002361958.

"Identity-Theft Case the Latest in a Series; Consumers'

Vulnerability to Fraud Rises." *The Washington Times*, February 22, 2005, C07. http://www.questia.com/PM.qst?a=o&d=5008729700.

Lacey, David, and Suresh Cuganesan. "The Role of Organizations in Identity Theft Response: The Organization-Individual Victim Dynamic." *Journal of Consumer Affairs* 38, no. 2 (2004): 244+. http://www.questia.com/PM.qst?a=o&d=5008625643.

Linnhoff, Stefan, and Jeff Langenderfer. "Identity Theft Legislation: The Fair and Accurate Credit Transactions Act of 2003 and the Road Not Taken." *Journal of Consumer Affairs* 38, no. 2 (2004): 204+. http://www.questia.com/PM.qst?a=o&d=5008649453.

Long, Wayne S. "Social Security Numbers Issued: A 20-Year Review." *Social Security Bulletin* 56, no. 1 (1993): 83-86. http://www.questia.com/PM.qst?a=o&d=5000191380.

Mann, Charles C. "Homeland Insecurity: A Top Expert Says America's Approach to Protecting Itself Will Only Make Matters Worse. Forget "Foolproof" Technology-We Need Systems Designed to Fail Smartly." *The Atlantic Monthly*, September 2002, 81+. http://www.questia.com/PM.qst?a=o&d=5002486137.

Marine Corps Order P5211.2B, "The Privacy Act of 1974," September 4, 1997.

Sipe, Jeffrey R. "Social Security Information: Privacy Issues Continue to Prompt Debate across the Country." *Insight on the News*, December 1, 1997, 40. http://www.questia.com/PM.qst?a=o&d=5000511332.