SMALL WARS JOURNAL

smallwarsjournal.com

The Military's Cultural Disregard for Personal Information

by Gregory Conti, Dominic Larkin, David Raymond, and Edward Sobiesk

Identity theft is not simply an inconvenience; it can lead to long-term financial and legal difficulties for individuals and families. In forward-deployed locations such as Iraq and Afghanistan, the distraction caused by identify theft can directly affect combat readiness as service members attempt to recover from these crimes. What makes matters worse it that Soldiers, Sailors, Airmen, and Marines face an increased likelihood of being targeted due to the manner that many military organizations treat individuals' Social Security numbers, dates of birth, and other Personally Identifiable Information (PII). There are numerous recent examples of deployed service members being victims of identity theft [1,2,3].

The time has come for the United States military to enforce a culture that respects PII and to discontinue use of the Social Security number as the primary means of tracking its personnel. We advocate the return to a service number system. The military previously used a service number system, but began replacing it in the late 1960's with Social Security numbers.[4] The impetus for the change stemmed from Executive Order 9397 which directed Federal agencies to use the Social Security number as an identifier to provide a single numerical identification system for Federal employees [5,6]. What authorities failed to envision at the time was how using the Social Security number as both a unique identifier for the Internal Revenue Service, which led to the use of SSNs across the financial spectrum to include banks, mortgage lenders, credit reporting agencies, etc., and as an employee identifier would lead to easy access to, and potentially widespread abuse of, this critical piece of PII. The result was a well-intentioned, but misguided, policy. In an era when an individual's Social Security number and date of birth have become the keys to identity theft, the ubiquitous use of the Social Security number by the military services is reckless. The problem is compounded by an uninformed, sometimes cavalier, culture and attitude surrounding the protection of PII that is common in the military.

While recently updated policy documents created at the most senior levels of the military services do exist [7,8,9,10], there is a significant disconnect between this high level policy and

[1] "Police: Man stole identity of deployed GI," The Army Times, 18 Aug 2010. Available online at http://www.armytimes.com/news/2010/08/ap-army-police-charges-stolen-identity-soldier-081710/

[2] "NYPD: ID Theft Ring Victimized Soldiers." Fox Network, 17 June 2010. Available online at http://www.myfoxny.com/dpp/news/local_news/staten_island/nypd-id-theft-ring-victimized-soldiers-20100616-akd

[3] "Fraudsters Claim a Red Cross Connection in New Phishing Scam." Press Release. Federal Trade Commission, 20 June 2007. Available online at http://www.ftc.gov/opa/2007/06/redcross.shtm

[4] The Army and Air Force transitioned to the Social Security number in 1969, the Navy and Marines in 1972 and the Coast Guard in 1974.

[5] Franklin D. Roosevelt. Executive Order 9397. 22 November 1943.

[6] Kathleen Swendiman. The Social Security Number: Legal Developments Affecting Its Collection, Disclosure, and Confidentiality. Congressional Research Service Report for Congress, RL30318, 21 February 2008.

[7] Defense Privacy and Civil Liberties Office. Available online at http://privacy.defense.gov/

the requisite culture required for proper protection of PII in practice. As a result, the military services lag a decade or more behind best practices found in other sectors of government, industry, and academia in the proper use and handling of PII. While positive progress has been made by the services, such progress is slow, ad-hoc, frequently ignored, and overshadowed by the common usage of the Social Security number as a way of tracking and identifying individuals. The systemic leakage of personal information in day to day operations, and a pervasive attitude of disregard for personal privacy is unsettling. Such issues are not tolerated outside the military - the time for substantive change within the military has arrived.

The problem of PII use has broad implications because the impact is felt by uniformed service members as well as government civilians, family members, and contractors, all of whom are compelled to disclose their Social Security number and incur the risk that it will be further disclosed, intentionally or unintentionally, without their knowledge or consent. The Federal Trade Commission, the United States Government's lead agency in preventing identity theft, states "Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give your Social Security number only when absolutely necessary, and ask to use other types of identifiers." [11] This guidance is impossible to follow within the military given the pervasive and compulsory use of the Social Security number.

There are some who believe that disclosing one's Social Security number or birth date is harmless, however, this view is patently incorrect. An individual's Social Security number combined with their date of birth provides access to one's identity. Scammers, identity thieves, and other criminals can use this information to commit a wide variety of crimes including opening new credit card accounts, generating credit reports, taking over existing accounts, or as a way to shield their true identity when arrested for a crime. There is even a recent trend where criminals will use the Social Security number of children as a means of stealing an untainted credit history [12].

Fixing the damage caused by identity theft is imperfect, stressful, expensive, and time consuming. Accounts must be closed and credit reports fixed through long and painful processes. Innocent individuals are subject to harassment by collection agencies. The cost is high in terms of time and frustration. The problem is magnified when an individual is deployed, allowing much damage to occur without their knowledge, or if known, serves to place additional stress on already strained families. Unlike a password which can be routinely changed, our Social Security number and date of birth are meant to be with us for life.[13] Thus, disclosure of this information places us at risk for life; in fact some identity theft even occurs after death, creating immense problems for surviving family members.

[8] United States Army Records Management and Declassification Agency. Available online at https://www.rmda.army.mil/organization/pa.shtml

[9] Air Force Force Privacy Act. Available online at http://www.privacy.af.mil/

[10] Department of the Navy Chief Information Officer – Privacy. Available online at http://www.doncio.navy.mil/TagResults.aspx?ID=36

[11] "DETER: Minimize Your Risk - Deter, Detect, Defend, Avoid ID Theft." Federal Trade Commission. Available online at http://www.ftc.gov/bcp/edu/microsites/idtheft/consumers/deter.html

[12] "Identity Theft and Children." Fact Sheet 120, Identity Theft Resource Center, 5 December 2009. Available online at http://www.idtheftcenter.org/artman2/publish/v_fact_sheets/Fact_Sheet_120.shtml

[13] It is, in fact, possible to get a new SSN, but it is not easy. According to the Social Security Administration's Office of the Inspector General, "[u]nder certain circumstances, SSA may assign you a new SSN if, after making all efforts to resolve the problems caused by someone else's misuse of your SSN, you are still being disadvantaged by the misuse." The Inspector General further states that "[t]here is no guarantee that a new number will resolve your problem."

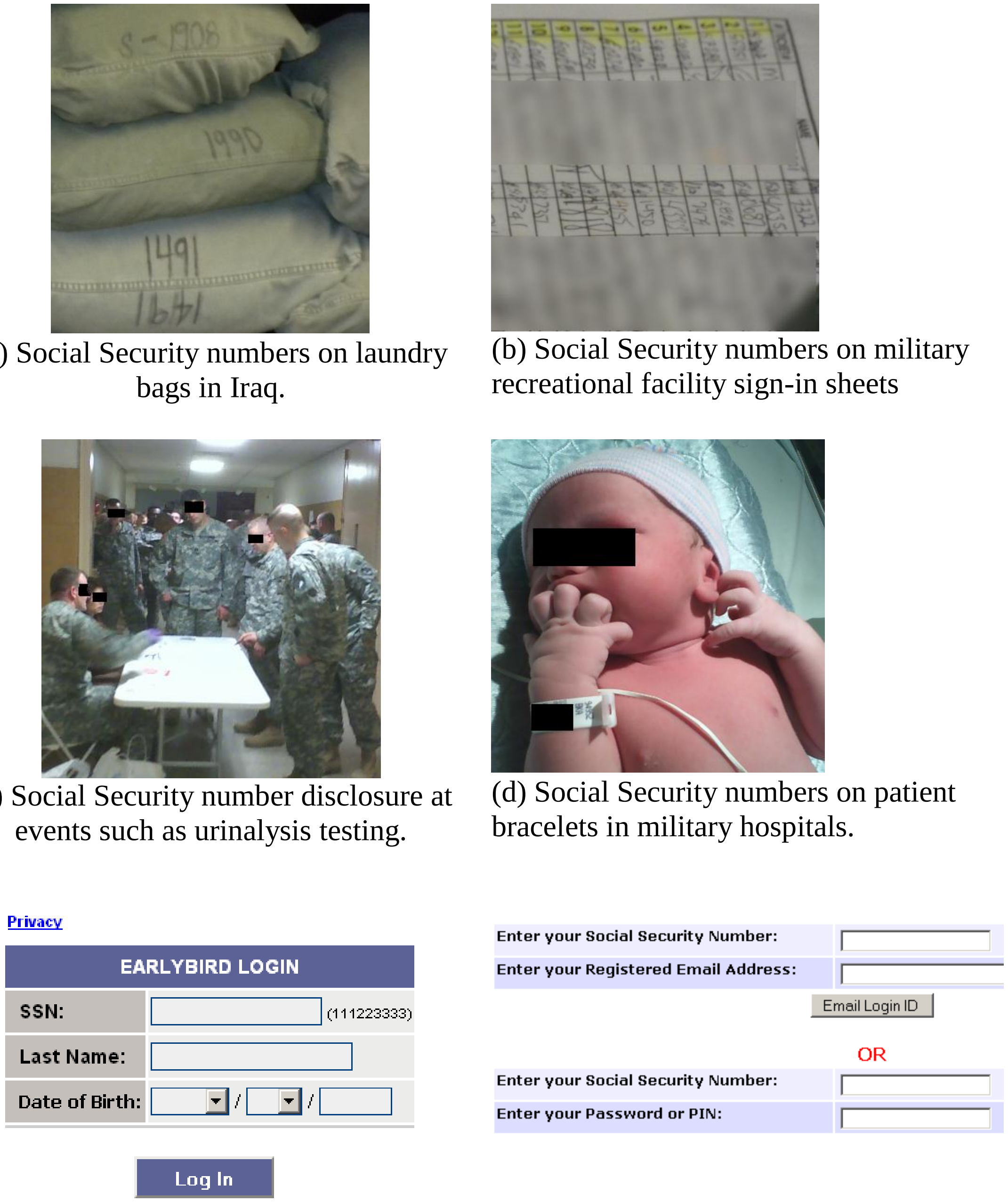
This article outlines the problem by illustrating the common use of the Social Security number as a unique identifier and pseudo-password in the military services. We illustrate the many ways, both large and small, that PII continues to be abused, as well as common misperceptions. We conclude with actionable solutions that will help correct the problem.

Examples of PII Misuse

It is easy to find examples demonstrating the widespread misuse of the Social Security number and other PII by the military. Consider the following obvious examples.

- Social Security numbers and dates of birth are exposed to foreign customs officials when traveling on official orders.
- Social Security numbers are exposed, all or in part, to contracted transportation companies and truck drivers during military moves.
- Virtually every Department of Defense form requires the Social Security number. Privacy Act statements on these forms typically dictate that disclosure is required.
- Many organizations create unofficial local forms and databases mandating disclosure of the Social Security number, with or without a Privacy Act statement.
- Dependent identification cards put the military sponsor's full Social Security number in the hands children as young as 10 years old.
- Many official and unofficial military administrative processes require service members to send unencrypted paperwork, such as leave requests and travel vouchers, containing Social Security numbers across the Internet. These forms are then stored, unencrypted, on myriad computers.
- Some military organizations use portions of Social Security numbers in email addresses and as computer user names.
- The Social Security number is stamped in steel on an individual's dog tags. Secure destruction of these tags is nearly impossible.
- Personnel in Iraq and other forward-deployed locations are required to put their Social Security number on checks to be cashed, write the last four digits of their Social Security number on laundry bags and when filling in gymnasium, Internet Café, and recreational facility sign-in sheets. Customer friendly local nationals working in laundry facilities have proudly memorized these numbers to provide faster, personalized service.
- Until recently, a Service Academy Alumni Association published books listing all graduate's dates of birth. Copies are available on Ebay.
- Service members, and their family members, frequently provide their Social Security number-laden military identification card to merchants, clerks, and night club bouncers for military discounts or as proof of age.
- Service members in Iraq, Afghanistan, and other foreign countries must show their military identification card to locally contracted, foreign national security guards to gain entrance to dining halls and other facilities, again disclosing their SSN and date of birth.

As these above examples and those in Figure 1 illustrate, the Social Security number, date of birth, and other PII are widely used, and widely disclosed, through the day to day activities of the military.


(a) Social Security numbers on laundry bags in Iraq.

(b) Social Security numbers on military recreational facility sign-in sheets

(c) Social Security number disclosure at events such as urinalysis testing.

(d) Social Security numbers on patient bracelets in military hospitals.

Privacy

EARLYBIRD LOGIN

SSN:	(111223333)
Last Name:	
Date of Birth:	/ /

Log In

Enter your Social Security Number:	
Enter your Registered Email Address:	

Email Login ID

OR

Enter your Social Security Number:	
Enter your Password or PIN:	

(e) Many military websites authenticate users using the Social Security number.

(f) The DoD website MyPay requires users who forget their Login ID to disclose their Social Security number.

Figure 1: The military culture is one of widespread compulsory Social Security number disclosure.

Common Misconceptions

The problems described in the previous section are compounded by common misconceptions surrounding how the military safeguards and employs personal information.

Myth #1: Military Data Does Not Spill

Despite efforts to the contrary, the military leaks personal information on a daily basis. Information, especially digital information, is slippery, and once spilled it is all but impossible to clean up the mess.[14] An example of a recent large-scale breach is the massive disclosure of classified documents by the Wikileaks website, which has caused serious damage to the United States war effort in Afghanistan [15]. Another massive data spill was the theft of a database containing the PII of 26.5 million U.S veterans from the *home* of a Department of Veterans Affairs employee [16]. Other examples include the theft of hard drives containing enrollment and claim files for 550,000 beneficiaries from a Tricare facility in a Phoenix, Arizona office park [17] and when a former U.S. Navy Petty Officer at a Fort Worth, Texas Joint Reserve Base compromised the identities of 8,000 sailors and used the information to steal more than $1 million via fraudulent checks and identification cards [18]. The military and its supporting agencies have suffered a litany of data spills, some accidental, others deliberate. All are irreversible and every one occurred despite existing policies and procedures designed to protect PII.

Large data spills such as these are complemented by myriad other smaller leaks, such as when individual service members and their families disclose personal information via social networking sites such as Facebook. Information such as hometown, hobbies, pets, favorite sports teams, and maiden names may appear innocuous on a web page but are very valuable to attackers seeking to bypass Knowledge Based Authentication systems found on Army Knowledge Online and other websites. For example, the Yahoo email account of former Alaskan governor Sarah Palin was hacked by using publically available information to reset her password [19]. Similarly, service members and their families are frequently targets of information harvesting phishing emails both at home and at work, and are tricked into disclosing sensitive information. Because of the widespread use of the Social Security number on most military paperwork, many personal computers of service members and their families contain PII in countless locations. Additional PII is stored when these computers are used to contact official websites because PII disclosure is necessary to log on. At the same time, personal computers can become infected with malicious software such as Trojan Horse applications and keystroke loggers, which capture and surreptitiously exfiltrate PII as legitimate users fill in military

[14] Data breaches are an ongoing problem for both the Government and private sectors, for a comprehensive listing see the Privacy Rights Clearinghouse's Chronology of Data Breaches (www.privacyrights.org/data-breach).
[15] "Afghanistan war logs: the unvarnished picture." The Guardian, 25 July 2010. Available online at http://www.guardian.co.uk/commentisfree/2010/jul/25/afghanistan-war-logs-guardian-editorial?intcmp=239
[16] Linda Rosencrance. "Active-duty troop information part of stolen VA data." Computer World, 6 June 2006. Available online at http://www.networkworld.com/news/2006/060606-active-duty-troop-information-part-of.html?nwwpkg=slideshows
[17] Tom Philpott. "Tricare files stolen from Central Region." Stars and Stripes, 26 December 2002. Available online at http://www.stripes.com/news/tricare-files-stolen-from-central-region-1.560
[18] Scott Gordon. "Military ID Theft Ring Steals More Than $1 Million, Police Say." Dallas-Fort Worth NBC, 13 November 2008. Available online at http://www.nbcdfw.com/news/local-beat/US-Military-Targeted-in-North-Texas-ID-Theft-Ring.html
[19] Bill Poovey. "Palin Set to Take Stand in Tenn. Hacking Trial." Associated Press, 21 April 2010. Available online at http://abcnews.go.com/Technology/wireStory?id=10433814

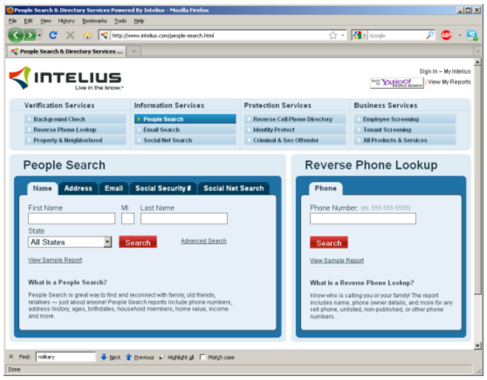
paperwork and visit official military websites. Every few months we hear news of scams where families, retirees, and service members are contacted by criminals seeking to elicit sensitive personal information. We argue that because of the widespread use of the Social Security number and other personal information these individuals are desensitized to its importance, making them ripe targets for such scams. Accidents can and will happen, and it is impossible to protect information from all disclosure, however, the best solution is to minimize the collection and use of personal information, process it securely, and destroy the information when no longer needed.

Myth #2: A Birth Date and Social Security Number Cannot be Guessed

When we randomly choose a password that is, say, 9 characters long, there are 10^{12} to 10^{16} possible results, depending on the use of upper and lower case characters, numbers, and common symbols. Unfortunately, the Social Security number is no password. We change our passwords every three to six months, but our Social Security number is with us for life. Far from being a 9 digit random number with a billion possibilities, parts of a Social Security number are based on easily guessable patterns related to location and date of birth. In fact, two Carnegie Mellon University researchers found that they can reliably guess the first five digits of the Social Security number given only those two pieces of information [20]. The researchers state that the relatively hard part of the problem is guessing the four digits of the Social Security number (often called the "Last 4"), which may take them several hundred tries. Given that we in the military divulge our Last 4 when signing out a basketball in Iraq and have it stenciled on the bottom of our laundry bags, we assume that guessing the Last 4 for service members is less of a problem.

The second major component for identity theft is the date of birth. Unfortunately, finding out an individual's date of birth is often trivial. Data broker websites such as Intelius, see Figure 2, make available birthdate lookup services, which include the birthdates of hundreds of thousands of service members, created from public records. To aid in the search, these sites list previous addresses of each individual. Because of frequent transfers between obviously military locations (Fort Benning, GA; Fort Leavenworth, KS; Fort Hood, TX; etc.), it is easy to zero in on military personnel and acquire their date of birth. These locations may also assist in determining location of birth if this isn't already disclosed on a Facebook page, a college yearbook, or through another data broker.

[20] Bob Sullivan. "Researchers say they can guess your SSN." Red Tape Chronicles, MSNBC, 6 July 2009. Available online at http://redtape.msnbc.com/2009/07/theres-a-new-reason-to-worry-about-the-security-of-your-social-security-number-turns-out-theyre-easy-to-guess--a-gro.html



What is a People Search?

People Search is great way to find and reconnect with family, old friends, relatives — just about anyone! People Search reports include phone numbers, address history, ages, birthdates, household members, home value, income and more.

What is a Reverse Phone Lookup?

Know who is calling you or your family! The report includes name, phone owner details, and more for any cell phone, unlisted, non-published, or other phone numbers.

Figure 2: Many online services, such as Intelius, allow easy discovery of an individual's date of birth, family members, and current and previous addresses.

Myth #3: The "Last 4" is to Safe to Use as a (1) Secret or (2) Public Identifier

We discussed in the previous section that determining the first five digits of an individual's SSN is not difficult. For someone trying to abuse your SSN, the hard part is determining the last four digits. Therefore, the belief that it is safe to disclose the last four digits of one's Social Security number or alternatively to use these digits as a form of password is fundamentally incorrect, but nevertheless common practice. For example, Figure 1(a) shows the use of the Last 4 as a means of sorting customer laundry in the Iraq Theater. Military and civilian customers are required to print their Social Security number in indelible ink on the bottom of their laundry bag. This practice, along with the requirement for forward-deployed Soldiers to divulge their Last 4 to use gyms, Internet café's, and other recreational facilities, further increases the risk of unauthorized disclosure of PII. In short, the Last 4, along with their name and signature is being widely disclosed as a matter of routine. At the same time, the Last 4 is being used by the Army and Air Force Exchange Service, AAFES.com, as a means to identify legitimate first-time customers, see Figure 3, under the weak assumption that the Last 4 is a secret known only to each legitimate customer. This disparity is indicative of the problem of the military's use of PII - on one hand PII is treated as a secret on the other it is disclosed and displayed in public locations.

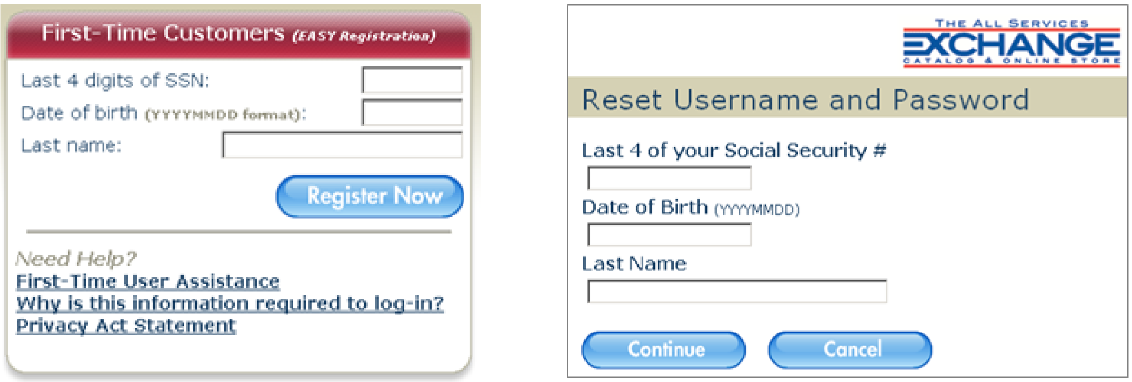

First-Time Customers (EASY Registration)
Last 4 digits of SSN:
Date of birth (YYYYMMDD format):
Last name:
Register Now
Need Help?
First-Time User Assistance
Why is this information required to log-in?
Privacy Act Statement
THE ALL SERVICES
EXCHANGE
CATALOG & ONLINE STORE
Reset Username and Password
Last 4 of your Social Security #
Date of Birth (YYYYMMDD)
Last Name
Continue
Cancel

Figure 3: The online Military Exchange system requires the user's Last 4, date of birth, and last name to create an account. The same information is required to reset an existing

account (right), potentially allowing existing accounts to be compromised by an attacker.

Myth #4: The Privacy Act Will Protect Privacy

The Privacy Act of 1974 is a code of fair information practices that regulates the collection, maintenance, use, and dissemination of personal information [21]. It states that it is unlawful for a government agency to deny any individual any privilege or benefit because of their refusal to disclose their Social Security number. However, it provides exceptions for agencies maintaining a "system of records" prior to 1975, which includes the Department of Defense. It also states that a government agency which requests that an individual disclose their Social Security number must "inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it." This provision results in the Privacy Act statements we see on official Department of Defense forms which explain the justification for disclosure of the Social Security number and the implications of our failure to do so. The Privacy Act statement was designed to inform individuals of their rights, but on most military forms it tersely states that disclosure is mandatory, or alternatively that disclosure is required to access a given service. Privacy Act statements on military forms frequently include threatening language, such as the DD2792 – Exceptional Family Member Medical Summary form whose Privacy Act Statement states that disclosure is:

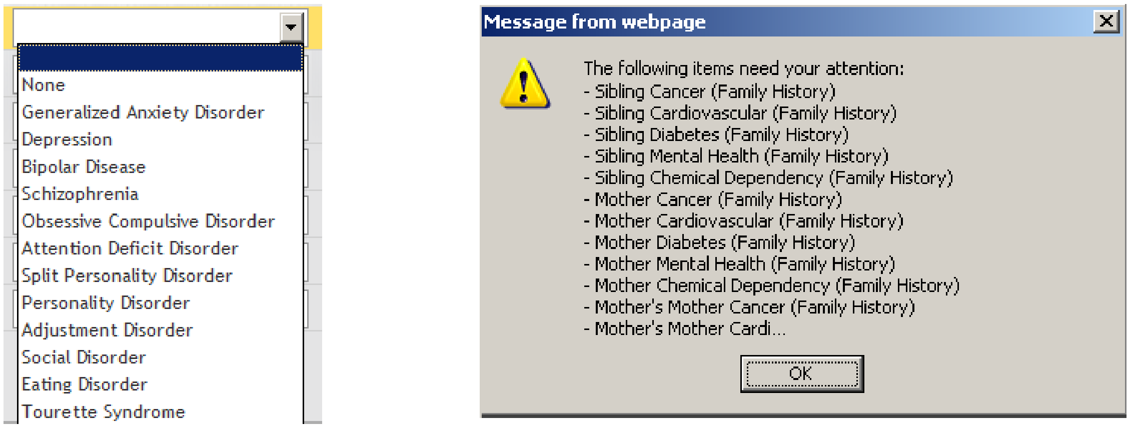
> Mandatory for military personnel; failure or refusal to provide the information or providing false information may result in administrative sanctions or punishment under either Article 92 (dereliction of duty) or Article 107 (false official statement), Uniform Code of Military Justice.

In addition to centrally distributed forms, which include Privacy Act information when necessary, the military employs local or unofficial forms and databases which frequently do not include Privacy Act information.

Because of the military's dependence on the Social Security number as a means of identifying its personnel, the Privacy Act statement has degraded from a helpful way of informing consumers of their rights to a method of mandating compliance. For many administrators and mangers there is no incentive to change this policy. However, at a minimum, we recommend creating revised privacy statements that are the result of careful consideration of what truly must be gathered and what is merely exploiting the military's too easily employed capability to dictate compliance. For example, Figure 4 depicts the MEDPROS website that every active duty Army Solider must visit as part of their mandatory annual health assessment process. In the Fall of 2009, the site did not contain any privacy policy, but at the same time forced users to disclose sensitive information, such as mental health conditions and drug use by parents and siblings. Abstaining from disclosing such information was not an option as service members were command directed to complete their physicals. The end result is that every Soldier in the Army was apparently compelled to disclose this information. Whether such

[21] "The Privacy Act of 1974." United States Department of Justice. Available online at http://www.justice.gov/opcl/privacyact1974.htm

compulsory disclosure is legal is an open question. For example, is it legal for an individual to disclose sensitive medical information about third parties without their consent? This could be just a well intentioned, albeit crudely executed, attempt to do the Army medical community's view of the right thing. However, to collect such sensitive information without even the benefit of a privacy policy raises important ethical and legal questions, particularly in the context of a military environment that requires strict adherence to orders. In addition, the fact that a privacy policy is an apparent afterthought on a website used to force disclosure of sensitive information from hundreds of thousands of service members on an annual basis is indicative of a culture with little regard for personal information.



The following items need your attention:
- Sibling Cancer (Family History)
- Sibling Cardiovascular (Family History)
- Sibling Diabetes (Family History)
- Sibling Mental Health (Family History)
- Sibling Chemical Dependency (Family History)
- Mother Cancer (Family History)
- Mother Cardiovascular (Family History)
- Mother Diabetes (Family History)
- Mother Mental Health (Family History)
- Mother Chemical Dependency (Family History)
- Mother's Mother Cancer (Family History)
- Mother's Mother Cardi...

Figure 4: The Army's Periodic Health Assessment Website is a service-wide requirement and compels Soldiers annually to disclose mental health and drug use information of parents and siblings without any privacy statement (Fall 2009). The site interface (left) did not allow any fields to be left blank and no option of abstention was available (right).[22] Completion of the form was a mandatory prerequisite for the actual medical assessment.

Myth #5: Individual Efforts to Fix Systemic Problems are Likely to Succeed

One might argue that to resolve the situations described in this paper, a service member need only inform the clerk, Non-Commissioned Officer, or Officer behind the desk that they are requesting information that they do not need to know, that they aren't protecting your information correctly, or that a given form is missing a Privacy Act statement. From our experience, this type of feedback is never well received and rarely understood. As a result, you won't get very far because they either do not understand what you are talking about, do not care, or aren't empowered to make a common sense decision. Even when you encounter a supportive individual, he or she will also fight against the tide of the larger systemic problem. For example, when one of the authors did not wish to disclose the health history of his parents and siblings, the doctor was supportive, but the doctor's interface into the online Periodic Health Assessment system required this information to complete the physical. When considering the bigger picture, the military excels at compelling compliance and hence service members are people who are expected to follow orders. Explaining to a peer, senior, or junior service member who is just trying to do their job why you won't provide your SSN or other PII will likely not have a

[22] This image has been modified slightly for clarity.

positive outcome, despite the legitimacy of your complaint. Top-down driven change to culture and processes need to come first. To try otherwise (as we have tried) is an exercise in futility.

Myth #6: People Will Follow Confusing and Unenforced Policy and Procedures

Although the military services possess extensive policies covering the protection of PII, we argue that while these policies provide legal protection for their associated bureaucracies and give the appearance of action, they fail to facilitate the requisite cultural change and do not provide meaningful protection for service members and their families during day to day operations. If you think we are off the mark, take a look through your office recycling bin (we have) and you will find out how well your organization is protecting sensitive information. If you don't like what you find, a simple email restating policy will not have any noticeable effect. A good example is ALARACT 138/2006 dated 21 July 2006 – "Army Personnel Responsibility for Safeguarding Personally Identifiable Information" which directed that Department of Defense personnel should:

> Take such actions, as considered appropriate, to ensure that personal information contained in systems of records, to which they have access to or are using incident to the conduct of official business, shall be protected so that the security and confidentiality of the information is preserved.

It is difficult to determine the extent that this email was followed, but we expect that it was largely ignored because people will skirt policy to accomplish their short term objectives, particularly when they do not understand the broader consequences. Blanket emails about PII security are essentially treated as SPAM and are ignored as are most policy memorandums generated at higher headquarters. Substantive change requires cultural improvements and engaged leadership at all levels. As with any policy, privacy regulations are only effective when they are widely and easily understood and enforced. We would argue, based on the many examples already offered, that this is simply not the case with current policy.

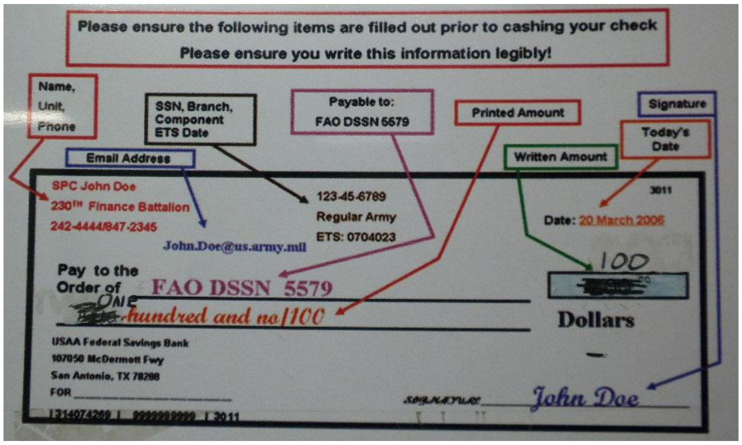
Some Positive Progress

It isn't all bad news, though, as the military has made some positive progress. We haven't required service members (and their families) to write Social Security numbers on checks for years (although, this practice apparently isn't completely extinct; see Figure 5). We aren't naively posting promotion lists, along with Social Security numbers, on the Internet nor are we placing Leave and Earning Statements on desks with the Social Security number in plain view. We routinely wipe all data from hard drives before disposal and only rarely see thumb drives containing sensitive data for sale at markets in combat zones. Some personnel records have had the full Social Security number converted to the Last 4 in service human resources databases. Also, the Veterans Administration has made a concerted effort to reduce (not eliminate) the use of SSNs through their Social Security Number Reduction Effort, begun in May 2007 [23].

However, despite this progress, the underlying problem still remains - the widespread use of the Social Security number and a casual attitude, at best, toward personal information. To

[23] "Social Security Number Reduction Effort," United States Department of Veterans Affairs. Available online at http://www.privacy.va.gov/ssn.asp

solve the problem we must move beyond localized, slow, and ad hoc improvements toward comprehensive, systemic, and cultural solutions.



Please ensure the following items are filled out prior to cashing your check

Please ensure you write this information legibly!

Name, Unit, Phone

SSN, Branch, Component ETS Date

Payable to: FAO DSSN 5579

Printed Amount

Signature

Today's Date

Email Address

Written Amount

SPC John Doe
230TH Finance Battalion
242-4444/847-2345

John.Doe@us.army.mil

123-45-6789
Regular Army
ETS: 0704023

3011

Date: 20 March 2006

Pay to the Order of FAO DSSN 5579

100

ONE hundred and no/100 Dollars

USAA Federal Savings Bank
107050 McDermott Fwy
San Antonio, TX 78288
FOR

SIGNATURE John Doe

1314074269 | 9999999999 | 3011

Figure 5: In Spring 2010, the Victory Base Complex Finance Office (Iraq) still mandated the use of the Social Security number on checks.

Solutions

We don't need quick fix solutions that just treat the symptoms -- a legalistic and chastising email sent out to the entire force is insufficient. Nor should the services muddle along in the current status quo. Instead we need widespread, systemic changes to the culture and processes surrounding the use of personal information, and these changes need to be embraced and enforced by Commanders at every level. Some of the changes we suggest are inexpensive and easy to implement, others are expensive and will require a longer term focus. However, the implications of information disclosure on personnel, their families, and our operational missions dictates that solutions are necessary, even if they are inconvenient for those benefiting from the current promiscuous status quo.

Broadly Employ a Service Number System, Protect the SSN

The biggest step, and we believe the most important, is for the Department of Defense to discontinue the use of the Social Security number, whether as a "secret" password or unique identifier, and institute a service number system. As noted earlier, the switch from service numbers to SSNs as the unique employee identifier for DoD personnel was well-meaning, but misguided. The military's continued use of the Social Security number, while technically legal, is not the proper way ahead for protecting PII. A service number system gives each individual a unique identifier which accomplishes the same goals as today's widespread use of the Social Security number, but without the risks associated with the widespread disclosure of SSNs. Under such a system, Social Security numbers can be stored in carefully guarded locations and used only when absolutely necessary, for example when reporting income to the Internal Revenue Service. Day to day operations can be conducted using the far more safe service number, because the service number cannot be directly used for identify theft. In circumstances that require authenticating individuals, we should leverage the existing Common Access Card infrastructure as a way to authenticate users instead of the using the Social Security number and date of birth. This transition may sound difficult, but many organizations across academia, industry, and government have demonstrated that it is both necessary and possible to avoid the use of sensitive PII for day to day operations. For example, the United States Coast Guard has already made a transition to an Employee Identification Number system in an attempt to safeguard the Social Security number and reduce the threat of identity theft [24].

Better Understand the Problem

An important step in addressing the prevalence and culture of PII issues within the military is to more deeply understand the problem. It is useful to think in terms of the collection, usage, transmission, storage and destruction of sensitive information. We should analyze when and where PII is being collected, how is it being used, how it is being transmitted and stored, and how is it being destroyed, if ever, when no longer needed. As part of this analysis, we recommend continued study into the depth and breadth of PII utilization including usage on paper forms, official websites, and databases. We acknowledge that there are ongoing DoD efforts in this area, but stress that such work must study the *culture* of PII usage and disclosure in day to day activities, as well as prevalence of identity theft across the military and civilian workforces, their families, retirees, and even affiliates such as contractors and unions. These insights will yield an understanding of what is being done well and what is being done poorly and will help focus subsequent efforts.

Change Culture and Raise Awareness

A key solution is raising awareness to the importance of privacy and changing the promiscuous culture of the services regarding personal information. The services deeply understand the importance of Operations Security (OPSEC) and are making solid progress in teaching Information Assurance (IA) and computer security principles. We can leverage this knowledge to help inform the workforce and their families about PII and privacy. Again, the services have made some progress in this area, but we recommend that they continue to look for opportunities to educate service members particularly through existing IA and OPSEC training programs. We should also exploit work being done by the Federal Trade Commission who make a wide variety of training materials available for free on the Web [25].

Changing the culture must include widespread application and enforcement of existing DoD and service element privacy policies. A key component to this solution is privacy officials down to battalion, squadron or equivalent levels. While some services, have policy mandating these positions as additional duties, the current status quo indicates that these individuals are currently not making a significant difference. Importantly, these officials should be empowered to find and recommend fixes to local policies and procedures that could lead to the abuse of PII, much like unit intelligence officers are empowered to enforce rules that keep classified data secure. Furthermore, there must be command emphasis placed on securing PII at all levels. This goes beyond simply enforcing service and DoD policy, it is an example of taking care of Soldiers that will be appreciated if the risks associated with PII leakage are clear.

[24] "About Employee ID Numbers." United States Coast Guard, 13 June 2000. http://www.uscg.mil/ppc/ps/general/about_employee_id_numbers.htm

[25] "Deter, Detect, Defend. Avoid ID Theft." Federal Trade Commission. Available online at http://www.ftc.gov/bcp/edu/microsites/idtheft/

Change will not occur overnight, but raising awareness and changing the military's culture will help eliminate some problems before they occur, lessen the impact of the issues that manifest problems, and are essential components of any systemic solution.

Make Privacy Easy

Let's face it, people are busy. Even if people are aware of the importance of privacy we still need to make the process easy. For example, because of the widespread use of the Social Security number on most Department of Defense and service forms, many personnel handle personal information of others on a day to day basis. Where is their nearest shredder?[26] Is it under their desk or down the hall? Is a shredder available at all? Will the shredder handle compact disks? If there isn't a capable shredder readily available, chances are that personal information will end up in an unsecured recycling bin or trash can.

Electronic forms are also increasingly common, as is their widespread dissemination via email for legitimate purposes. Email is an incredibly powerful means of communication, but without encryption it is inherently insecure. So why don't people use encryption? We argue encryption isn't employed because the current system has had a history of being difficult to use, and we lack the habit of using it. The best forms of security silently protect users without requiring manual intervention or deep technical understanding. Consider the secure mode of your browser, during sensitive online activities such as banking, the browser quietly encrypts its communications and displays a small padlock to the user as an indicator. This ease of use has fueled the immense growth in eCommerce on the World Wide Web. We need to develop and consistently employ *usable* systems that allow easy, secure, and reliable email communications across the Department of Defense enterprise.

Another example is providing people an easy and well advertised way to report privacy issues. While a local administrative officer may be able to handle routine privacy issues, from our experience, systemic problems require senior points of contact who understand privacy implications and privacy law, and, more importantly, have the power to facilitate organizational change.

Appoint Dedicated DoD and Service Component Chief Privacy Officers

Without empowered, resourced and visible senior leadership, progress in protecting PII will occur slowly. Over the past decade, private industry recognized this fact and has been appointing dedicated Chief Privacy Officers charged with the responsibility of overseeing privacy programs and serving as ombudsman for privacy issues within their companies. In 2000, IBM appointed their first Chief Privacy Officer and other major organizations have followed suit, including Google, Facebook, Adobe, and MySpace [27]. The Department of Homeland Security (DHS) has an active privacy office and Chief Privacy Officer. Created in 2002, the DHS privacy office was the first statutorily mandated privacy office of any federal agency. Their mission is to preserve and enhance privacy protections and promote the transparency of

[26] It is important to note that not all shredders are created equal. Documents sent through strip cut shredders can be easily reassembled via manual or computer-assisted means. See "Piecing Together the Dark Legacy of East Germany's Secret Police" in Wired issue 16.02 for an excellent example. Cross-cut shredders are a much better, but not infallible, choice.

[27] Joe Wilcox. "IBM appoints chief privacy officer." CNET News, 28 November 2000. Available online at http://news.cnet.com/IBM-appoints-chief-privacy-officer/2100-1001_3-249135.html

Homeland Security operations [28]. While the Department of Defense and the military services have created privacy offices and privacy officials, such as those found in the DoD Privacy Office (privacy.defense.gov) [29], we recommend providing increased resourcing to these programs and the formal appointment of DoD and service component officials, using the title of Chief Privacy Officer, who possess the influence and status to energize substantive and rapid progress, and to serve as a clear indicator of organizational commitment similar to that of DHS, Google, and Facebook.

Adopt Best Practices from Government Agencies and the Private Sector

Outside the military, the need to protect PII is not a recent discovery. Both the private sector and government agencies have developed best practices that the military can adopt. In particular, the Federal Trade Commission has deeply studied the problem of identity theft and made available a great deal of helpful information to consumers and businesses on best practices for protecting PII [30].

Based on available artifacts it appears that small pockets within the military hierarchy possess a cogent understanding of best practices [31], but we believe such resources are not well known nor well applied in day to day activities. While it is beyond the scope of this article to list all possible best practices, we do recommend broadly disseminating this information to DoD-affiliated personnel and deeply embeding these practices into our workflow processes and organizational culture.

Conclusion

The United States military is at least a decade, perhaps two decades, behind best practices in the protection of personal information of its employees and family members. The time is now to move from the Social Security number system to a safer and more secure service number system -- many other large organizations have already successfully made the switch. The military has leaked millions of records through theft, ignorance, and apathy. The future portends an even higher risk environment as powerful mobile devices, which may be easily lost or stolen, will be frequently used to process, communicate and store personal information. The end result is that service members and their families are burdened with a work environment that shows little regard for their personal information, leaving them vulnerable to identity theft, fraud, and other malicious activities. Once disclosed, history has shown that it is impossible to put the genie back in the bottle. Service members, their families, and their units' military preparedness and combat effectiveness all will pay a price for decades to come. A key component of a solution is quarantining the Social Security number to rigorously secured databases and use of a service number for all operations except when absolutely required, such as financial transactions. This effort must be complemented by cultural change that instills in service members, especially

[28] Chief Privacy Officer Biography: Mary Ellen Callahan. Department of Homeland Security, 29 July 2010. Available online at http://www.dhs.gov/xabout/structure/bio_1236273286409.shtm

[29] DoD Component Privacy Points of Contact. Department of Defense Privacy Office Website, 26 September 2010. Available online at http://privacy.defense.gov/dpo_points_of_contact.shtml

[30] "Protecting Personal Information: A Guide for Business." Federal Trade Commission. Available online at http://www.ftc.gov/bcp/edu/pubs/business/idtheft/bus69.pdf

[31] United States Army Office of Information Assurance and Compliance, 28 August 2010. Available online at https://informationassurance.us.army.mil/training_education/index.php. Note that access is restricted to DoD personnel.

leaders, the importance of protecting the Social Security number, date of birth, and other sensitive information.

If we fail to keep our service members' PII safe then we are allowing our enemies a critical means for attacking us in the ever growing non-linear and unconventional battlefield. In the Gulf War, we defeated the 4th largest army in the world in a matter of days. For our enemy to be successful now they must find new ways to attack us, and we are giving them an easy attack vector with the current culture of promiscuous PII use and leakage. How effective would a battalion be in which more than half the Soldiers and all the key leaders are facing eviction, home foreclosures and automobile repossession because their financial identity is in the hands of terrorists or criminals. We live in an age where an individual can cross international borders and geographical boundaries many times a second using the Internet. With foreign custom agents and laundry workers potentially collecting our Soldiers' Social Security numbers and other PII, it may be too late to prevent this kind of attack, but by quickly switching to a service number we can limit those exposed to it in the future.

Lieutenant Colonel Gregory Conti is a Military Intelligence Officer and Director of West Point's Cyber Security Research Center. He holds a BS from West Point, an MS from Johns Hopkins University and a PhD from the Georgia Institute of Technology, all in Computer Science. He is the author of Security Data Visualization (No Starch Press) and Googling Security (Addison-Wesley) as well as numerous articles covering information security, online privacy, and cyber warfare. He has deployed in support of Operations Desert Shield, Desert Storm and Iraqi Freedom.

MAJ Dominic Larkin is a Field Artillery Officer and Instructor in West Point's Department of Electrical Engineering and Computer Science. He holds a BS from Troy State University and an MS from the Georgia Institute of Technology. His research interests include computer science education, robotics, digital security and electronic privacy. He deployed in support of Operation Just Cause and Operation Iraqi Freedom.

LTC David Raymond is an Armor Officer and Assistant Professor in West Point's Department of Electrical Engineering and Computer Science. He holds a BS from West Point, an MS in Computer Science from Duke University, and a PhD in Computer Engineering from Virginia Polytechnic and State University. LTC Raymond's research interests include wireless sensor and mobile ad hoc networks, wireless network security, and online security and privacy. He has deployed in support of Operations Desert Shield, Desert Storm and Iraqi Freedom.

COL Edward Sobiesk is an Armor Officer and Director of West Point's Information Technology Program. He holds a BS in Computer Science from Winona State University, and an MS and a PhD in Computer and Information Sciences from the University of Minnesota. COL Sobiesk's research interests include electronic privacy, computer science & information technology education, computing ethical and legal considerations, and artificial intelligence. He has deployed in support of Operations Desert Shield and Desert Storm.

The views expressed in this article are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, the Department of Defense, or the United States Government.