YOUR SOCIAL SECURITY NUMBER OR YOUR LIFE: DISCLOSURE OF PERSONAL IDENTIFICATION INFORMATION BY MILITARY PERSONNEL AND THE COMPROMISE OF PRIVACY AND NATIONAL SECURITY

Rick S. Lear & Jefferson D. Reynolds*

* Jefferson D. Reynolds is the Environmental Counsel to Kirtland Air Force Base in Albuquerque, New Mexico. He is also a Major in the Air Force Reserve, previously assigned as an Operational Law Counsel to Special Operations Command, Europe (SOCEUR); Hamline University, J.D. (1990); George Washington University, LL.M (Environment) (1995). Rick S. Lear is a Major in the U.S. Army Judge Advocate General's Corps, was formerly assigned as Legal Advisor to SOCEUR, and is currently pursuing an LL.M. at the Judge Advocate General's School of the Army; University of Nebraska, J.D. (1994). The views expressed in this article are those of the authors and not the Department of the Air Force, Department of the Army, nor the Department of Defense.

I have no reason to suppose that he who would take away my liberty would not when he had me in his power take away everything else. And therefore it is lawful for me to treat him as one who has put himself into a state of war against me [and] kill him if I can . . . .[1]

I. INTRODUCTION

August 5, 1964, during one of the first sorties in Viet Nam, Lieutenant Junior Grade Everett Alvarez, Jr. was shot down by the North Vietnamese.[2] After ejecting from his plane, he was able to carry out one conscious thought: to get rid of the wedding band on his left finger. He knew that if the North Vietnamese had identified him as being married they would have had a tremendous psychological advantage over him.[3]

April 1, 2001, Lingshui Air Base, Hainan, during a routine reconnaissance mission in international waters, Navy Lieutenant Shane Osborn and his crew were forced to make an emergency landing on Hainan Island, China. During Lieutenant Osborn's detention and interrogation, the safety of his family was threatened in an attempt to force him to provide information.[4]

January 15, 2005, at an undisclosed location during the Global War on Terrorism, Sergeant First Class Timothy L. Greene is detained by transnational terrorists.[5] Fearing that his treatment will be harsh, he immediately provides his name, rank, date of birth and service number. At the same time he presents a Geneva Conventions Identification Card providing his full name and social security number.[6] He gives no further information about either himself or his family, but is hopeful he will receive humane treatment as a Prisoner of War (POW). Unfortunately, by complying with the laws of war, Sergeant First Class Greene has shared more private information about himself than any other POW or detainee before him.

Sergeant First Class Greene's dilemma is plausible given the capabilities of computer technology. Computer and Internet technology is developing at such an exponential pace, it is difficult to predict the ramifications on privacy or how it will affect national security many years

---

[1] *See* JOHN LOCKE, SECOND TREATISE OF GOVERNMENT § 18 (Richard Cox ed., 1982) (1689).

[2] EVERETT ALVAREZ, JR. WITH SAMUEL A. SCHREINER, JR., CODE OF CONDUCT 1 (1971).

[3] *Id.* at 7-8.

[4] SHANE OSBORN WITH MALCOLM MCCONNELL, BORN TO FLY 159-60 (2001).

[5] Sergeant First Class Timothy L. Greene is a fictional character.

[6] This article does not address the new Geneva Conventions Identification Card recently adopted by the Department of Defense containing a microchip of service related and private information. All service identification cards presently bear the service member's full name, social security number, rank, blood type and date of birth.

from now. There is no clear understanding of how this technology affects national security even now. Some trends, however, are unmistakable: 1) the volume of private information recorded, collected and distributed about people will increasingly expand; 2) the societal privacy conflict will become even more bitter; and 3) attempts to restrain surveillance, information collection and distribution will be intensified.[7] Privacy has been eroded for decades, and the advent of the information age only accelerates the process. In an article used by the Senate to review the Internet privacy problem, the author made a bold prediction:

> all these efforts to hold back the rising tide of electronic intrusion into privacy will fail. . . . [Twenty] years hence most people will find that the privacy they take for granted today will be just as elusive as the privacy of the 1970s now seems. . . . This will constitute one of the greatest social changes of modern times.[8]

Even worse, the U.S. Congress recognizes that the United States is one of the few modernized countries not providing comprehensive legal protection of private information.[9] The trend of failing to protect private information becomes even more unnerving when military personnel and national security are factored into the equation.

The potential for compromising a military member and national security while in POW status is significant due to the austere treatment and conditions suffered by the service member. The United States developed the Code of Conduct largely in response to the actions of Korean POWs.[10] Military members compromised during interrogations to the point of providing information on military operations or other information relating to national security pose a significant risk to the military and security of the United States. Tragically, it is the Code of Conduct, and the Department of Defense's implementation of the Geneva Convention Relative to the Treatment of Prisoners of War requiring POWs to reveal their social security number, which places virtually every private detail of a POW's life at the fingertips of their captors.

Appreciative that the Internet is truly wonderful technology, many of the good things in the world can be used as weapons absent careful observation. This article discusses the problem with the collection of private information by commercial industry and the threat this collection has to national security when networked with other Internet data banks.

---

[7] *Statement on Introduced Bills and Joint Resolutions*, 145 Cong. Rec. S14533-S14536 (November 10, 1999) (quoting *The End of Privacy*, THE ECONOMIST, May 1-7, 1999, at 15).

[8] *The End of Privacy*, *supra* note 7, at 15.

[9] *Statement on Introduced Bills*, *supra* note 7, at S14538.

[10] *Report of the Secretary of Defense's Advisory Committee on Prisoners of War*, POW, THE FIGHT CONTINUES AFTER THE BATTLE v-vii (1955).

Traditionally, the argument that private information should not be subject to disclosure is largely fought from a constitutional angle.[11] As private information collection grows and Internet use increases, Congress must consider the effects on national security. Although POWs are emphasized in this article because they are most at risk, all military members, government officials and even some government contractors are potentially compromised by the collection and distribution of private information over the Internet. Part II of this article discusses why the social security number was created and how it contributes to the demise of national security. Part III describes how POWs in captivity are vulnerable to conditions resulting in the disclosure of important information. Part IV illustrates the potential damage that can be caused with only a small amount of private information. Part V surveys the current legal framework protecting private information and how it falls short of protecting national security. Part VI reviews the European model for private information protection and legislation being considered by the U.S. Congress. Finally, the Conclusion of this article outlines practical and legal solutions to adequately protect both national security and personal privacy.

II. CREATION OF THE SOCIAL SECURITY NUMBER AND THE DEMISE OF NATIONAL SECURITY

A. *The Adoption of the Social Security Number as a National Identifier*

The Social Security Act was originally created to develop a system of social security numbers that would be used exclusively to monitor earnings and determine the amount of an individual's tax liability.[12] When it was enacted, politicians specifically commented that the numbers would not be used to implement a national identification system.[13] As the information age evolved, so did the use of social security numbers away from their original purpose. In 1943, President Roosevelt signed an Executive Order requiring all Federal agencies to adopt the social security number as a personal identifier to meet the need for a national identification sys-

---

[11] Stanley v. Georgia, 394 U.S. 557, 564-66 (1969); NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 460-63 (1958); Katz v. United States, 389 U.S. 347, 350-53 (1969); Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); Boyd v. United States, 116 U.S. 616, 627-30 (1886); Mapp v. Ohio, 367 U.S. 643, 656-57 (1961); Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965); Roe v. Wade, 410 U.S. 113, 152-53 (1973).

[12] *See* Bill Olds, *No Way to Stop the Spread of Social Security Numbers*, HARTFORD COURANT H3 (August 26, 2001), *available at* 2001 WL 25319587.

[13] Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L.Q. 461, 498-99 & n.98 (1999).

tem.[14] Although few agencies adopted the social security number as an individual identifier at the time,[15] the Civil Service Commission required all Federal employees to obtain a social security number for use as a personal identifier in 1961.[16] Then in 1962, the Internal Revenue Service adopted the social security number as a tax identification number for tax returns.[17]

On July 1, 1969, the Department of Defense ceased issuing serial numbers and adopted the social security number in its place.[18] The rationale for this shift was to implement the 1943 Executive Order, and to increase efficiency in personnel record administration.[19] In 1969, during an era where records were generated on typewriters and filed in cabinets, it would have been easy to conceive that the social security number would fill a void to increase efficiency for both government and commercial industry. As the need for a national identifier for American citizens evolved with information management and technology, the social security number was the logical choice because it was already in place. It is unlikely that such a system would have been adopted had anyone foreseen the creation of the Internet, the relative ease of obtaining private information over the Internet, and the potential damage it could have to an individual.

Further solidifying the use of the social security number as military identification, Section 3 of the Military Selective Service Act empowers the President to require every male American citizen and resident alien between the ages of eighteen and twenty-six to register for the draft.[20] Section 12(b) of that Act imposes criminal penalties for failure to register.[21] On July 2, 1980, President Carter issued a Proclamation requiring

---

[14] Exec. Order No. 9397, 3 C.F.R. 283-84 (1943-1948) (ordering federal agencies to use the social security number).

[15] *Use of Social Security Number as a National Identifier: Hearing Before the Subcomm. on Social Security of the House Comm. on Ways and Means*, 102d Cong. 23 (1991) (testimony of Gwendolyn S. King).

[16] Soc. Security Admin., *Social Security Number Chronology of History*, *at* http://www.ssa.gov/history/ssn/ssnchron.html (last visited Feb. 15, 2003) [hereinafter *History of Chronology*].

[17] Internal Revenue Code Amendments, Pub. L. No. 87-397, 75 Stat. 828 (1961) (codified as amended at 26 I.R.C. § 6109 (1999).

[18] *Army is Dropping Serial Numbers,* N.Y. TIMES, July 2, 1969, at 3. The Social Security Administration website indicates 1967 is the year that the Department of the Army adopted the social security number in place of registration numbers. *See History of Chronology*, *supra* note 16. The discrepancy of dates suggests a decision might have been made in 1967 to convert to the social security number, but implementation did not occur until 1969.

[19] *Id.*

[20] Selective Services Act of 1948, 62 Stat. 605, *as amended* 50 U. S. C. App. § 453.

[21] *Id.*

young men to register within thirty days of their eighteenth birthday.[22] Virtually all young men in the United States have registered with the Selective Service using a social security number for identification.[23]

Congress and the judiciary, in failing to maintain the original intent of the Social Security Act, have created a privacy nightmare jeopardizing the security of American citizens and national security. While there is no easy solution, the simple solution is to use one number for one purpose. An individual's social security number should be used solely for its original purpose of monitoring earnings and collecting taxes. An individual in the military, associated with the military, or otherwise likely to become a POW, should be issued a "serial number" as was the general practice as early as 1921.[24] Although likely subject to great resistance from private industry, commercial exploitation of the social security number in conjunction with other private information must be curtailed in order to provide protections to service members and national security.

B. *The Requirement for POWs to Provide a Social Security Number*

The Geneva Convention Relative to the Treatment of Prisoners of War (Geneva III) (GPW) sets forth the obligations of a capturing power to account for POWs.[25] Drafted soon after World War II, the GPW focuses primarily on more traditional forms of war with readily identifiable armies in the field.[26] Accordingly, the GPW is intended to provide protection to lawful combatants engaged in an international war or armed conflict.[27]

---

[22] Proclamation No. 4771, 3 C.F.R. § 82 (1981).

[23] Selective Service System Form 1, *at* http://www.sss.gov/IFR06.htm (last visited Mar. 24, 2003); *see also* Selective Service System Online Registration, *at* https://www4.sss.gov/regver/register1.asp (last visited Feb. 15, 2003).

[24] *Army is Dropping Serial Numbers, supra* note 18.

[25] Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3114, 75 U.N.T.S. 31 (entered into force Oct. 21, 1950); Geneva Convention for the Amelioration of the Condition of Wounded, Sick, and Shipwrecked Members of the Armed Forces at Sea, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3217, 75 U.N.T.S. 85 (entered into force Oct. 21, 1950); Geneva Convention Relative to the Treatment of Prisoners of War, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3316, 75 U.N.T.S. 135 (entered into force Oct. 21, 1950) [hereinafter GPW]; Geneva Convention Relative to the Protection of Civilian Persons in Time of War, *opened for signature* Aug. 12, 1949, 6 U.S.T. 3516, 75 U.N.T.S. 287 (entered into force Oct. 21, 1950).

[26] GPW, *supra* note 25.

[27] The GPW states that "the present Convention shall apply to all cases of declared war or any other armed conflict which may arise between two or more of the High Contracting Parties, even if the state of war is not recognized by one of them." *Id.* art. 2. The GPW also defines the persons entitled to POW protection. *Id.* art. 4.

The GPW contains three basic provisions regarding the identification and reporting requirements for POWs.[28] The obligations and binding effect of these provisions vary. The first of these, Article 17, requires the prisoner to provide only his "surname, first name, rank, army, regimental personal or serial number or equivalent information, and date of birth."[29] POWs must provide this information to the detaining power immediately after capture orally or by allowing the captor to view their identity cards or by answering questions in the prisoners' language.

During World War II, captured service members were required to give only their name and rank or regimental number.[30] The use of only one piece of identifying information was found to be wholly inadequate for identification purposes.[31] More information was required to adequately crosscheck and verify information given to the POW's own country.[32] Even at the time of the adoption of the GPW, there was some concern that giving information such as age and rank might be of military value.[33]

For identification purposes, a POW is only required to show an identity card to his or her captor.[34] The identity card constitutes proof that the owner is entitled to protections under the GPW.[35] Every party has a duty to "furnish the persons under its jurisdiction who are liable to become prisoners of war, with an identity card. . . ."[36] This includes not only military personnel, but also those civilians participating in the military operation, providing technical assistance or otherwise accompanying the armed forces.[37] To ensure civilians are provided proper treatment when

---

[28] Article 17 applies to the questioning of prisoners. *Id.* Article 70 lists the information given by the prisoner to his or her family and the Central Prisoner of War Information Agency. *Id.* Article 122 requires a national information bureau and describes the information to be reported by the detaining power to the Central Prisoners of War Information Agency. *Id.*

[29] *Id.* art. 17.

[30] 1929 Geneva Convention Relative to the Treatment of Prisoners of War, 27 July 1929, 118 L.N.T.S. 343 (providing that "[e]very POW is bound to give, if he is questioned on the subject, his true name and rank, or else his regimental number").

[31] JEAN S. PICTET, COMMENTARY: III GENEVA CONVENTION RELATIVE TO THE TREATMENT OF PRISONERS OF WAR 158 (1960).

[32] *Id.*

[33] *Id.*

[34] GPW, *supra* note 25, art. 18.

[35] PICTET, *supra* note 31, at 162

[36] *Id.* (quoting 1929 Convention Relative to the Treatment of Prisoners of War, *supra* note 30, art. 17).

[37] In defining those individuals to be treated as prisoners of war, the GPW states:

> Persons who accompany the armed forces without actually being members thereof, such as civilian members of military aircraft crews, war correspondents, supply contractors, members of labour units or of services responsible for the welfare of the armed forces, provided that they have received authorization from the armed forces which they accompany, who shall provide them for that purpose with an identity card . . .

captured, their possession of identification cards is critical. Given the requirement for a civilian employee or contractor to provide a social security number in the event of capture, the damage to the individual's privacy and risk to national security is still the same. As non-combatants not subject to the Code of Conduct, yet afforded the protections of a POW, the definitions and application of POW protections become difficult to construe for civilians. For these reasons, the GPW requires that persons whose status is in doubt receive the same protections as a POW until a competent tribunal determines their status.[38]

Interrogation of POWs is lawful, but coercion in any form is not.[39] What constitutes coercion goes beyond the scope of this article. Suffice it to say that based upon the American experience, defining the term "coercion" for purposes of the right against self-incrimination has been difficult, at best, under U.S. law; therefore, one cannot expect a definition under international law to be less troubling.[40] Herein lies an important distinction in the drafting of the GPW. The GPW defines "grave breaches" as:

> willful killing, torture or inhuman treatment, including biological experiments, willfully causing great suffering or serious injury to body or health, compelling a prisoner of war to serve in the forces of the hostile Power, or willfully depriving a prisoner of war of the rights of a fair and regular trial . . . .[41]

Parties are required to enact penal legislation for grave breaches of the GPW, but required only to suppress all acts other than grave breaches.[42] While threats made against the family members of POWs certainly constitute coercion, it leaves open the question of a grave breach.

There is no prohibition against telling a POW what is already known during interrogation. If an enemy knows of important information and wishes to share that knowledge with a POW, there is no prohibition against doing so. In fact, this is a routine interrogation technique that is used to confirm information gained from other sources, or to make the POW more compliant to the questions sought by the interrogator.[43] Imagine a POW being confronted not only with military information, but

---

GPW, *supra* note 25, art. 4(A)(4). For a discussion of potential issues that may arise concerning civilians accompanying the armed forces, see W. Hays Parks, *The Gulf War: A Practitioner's View*, 10 DICK. J. INT'L L. 393, 407-09 (1992).

[38] GPW, *supra* note 25, art. 5.

[39] *Id.* art. 17. (stating "[n]o physical or mental torture, nor any other form of coercion, may be inflicted on prisoners of war to secure information of any kind whatsoever. Prisoners of war who refuse to answer may not be threatened, insulted or exposed to unpleasant or disadvantageous treatment of any kind.").

[40] See Miranda v. Arizona, 384 U.S. 436 (1966) and its progeny.

[41] GPW, *supra* note 25, art. 130.

[42] GPW, *supra* note 25, art. 129.

[43] J.M. SPAIGHT, AIR POWER AND WAR RIGHTS 390 (3d ed. 1947) (1921).

information about the prisoner's home, family, financial history, or any other available private information.

What is important to note is that the GPW does not require an efficient, practical or nationally recognized identification number. Rather, the concern of the GPW is that the POW's own country is able to verify a POW's identity.[44] The requirement places upon the detaining power the burden of providing additional information to its enemy so the POW can be more adequately protected.[45] While a social security number meets this objective, it simultaneously provides too much information to even the most law-abiding of captors. A detaining power presently violates no U.S. or international law in developing a profile of a POW's private information from readily available Internet sources.

Sadly, the Department of Defense has yet to adopt changes which fully recognize the private nature of the social security number and the potential significance of revealing that number to captors. Since the Department of Defense stopped issuing "serial numbers" in 1969, the social security number of every service member has been printed on their military identification card and identification discs, or "dog tags." The military medical system also uses the social security number of the service member to verify eligibility for medical care of service members and their dependents. The practical implication is that family members memorize the social security number of their sponsoring service member out of necessity. Military records systems are nearly all maintained, accessed and verified by social security number. Every service member normally has in his or her possession, at any given time, the social security number of other members of his unit for one reason or another.[46] The end result of this proliferation of the use of the social security number in the military has been to generally make available the social security number of service members to society as a whole. Indeed, the Department of Defense has been forced to act on more than one occasion to protect service members from identity theft as a result of the widespread publica-

---

[44] PICTET, *supra* note 31, at 158.

[45] *Id.* at 159-61.

[46] All flight manifests, jump manifests, and many other unit operations rosters contain individual social security numbers of all members participating in the operation. See, for example, Department of the Army Form 1306: Statement of Jump and Loading Manifest (May 1, 1963), *available at* ftp://pubs.army.mil/pub/eforms/pdf/a1306.pdf which, when completed, contain the name and social security number of all personnel participating in an airborne operation. The form is frequently provided to all service members participating in the operation. Department of Defense Form 1610: Request and Authorization for Temporary Duty Travel of DoD Personnel (January 2001), *available at* http://www.dior.whs.mil/forms/DD1610.PDF, requiring the name and social security number of traveling service members. The form is frequently presented to foreign military and customs officials to verify identification and official travel.

tion of social security numbers.[47] Notwithstanding these concerns, no precautions have been taken to protect the release of service members' social security numbers from America's enemies.

III. THE DAMAGED PSYCHOLOGY OF A POW AND THE DISCLOSURE OF INFORMATION

Armies in the field have long used interrogation of POWs as an intelligence tool. During the American experiences in Korea and Viet Nam, POWs were used as propaganda tools.[48] It was the relatively low resistance of American POWs to interrogation methods and techniques during the Korean conflict that led to the development of Executive Order 10631.[49] Known as the Code of Conduct (Code), it instructs members of

---

[47] *See, e.g.*, Suzann Chapman, *Aerospace World*, AIR FORCE MAGAZINE, Feb. 2002, at 27 (stating that the "DoD now urges caution in filing official documents at local courthouses"). *See also* Dennis Blank, *Data from Federal Records Used to Commit Identity Theft*, 19 GOV'T COMPUTER NEWS, Oct. 2, 2000, at 8, *available at* http://www.gnc.com/vol19_no29/news/3046-1.html (reporting that "[o]ne Pennsylvania web site lists 4,800 officers' social security numbers . . ."). For information on the most recent military concern about identity theft see Tom Philpott, *Military Update, TRICARE Beneficiaries' Personal Information Stolen*, HONOLULU ADVERTISER, December 30, 2002, at 4B. A theft of computer hard drives from the military's managed care support contractor on December 14, 2002, was believed to be "'theft of information, pure and simple.'" *Id.* (quoting David J. McIntyre, Jr., president of TriWest, the managed care support contractor).

[48] P.O.W.; *The Fight Continues After the Battle, the Report of the Secretary of Defense's Advisory Committee on Prisoners of War* vi, 1-2 (July 29, 1955).

[49] Exec. Order 10631, CODE OF CONDUCT FOR MEMBERS OF THE ARMED FORCES OF THE UNITED STATES, August 17, 1955, was the original formulation for the Code of Conduct. It may be found in its current form at CODE OF CONDUCT TRAINING & EDUCATION (January 8, 2001), *available at* www.dtic.mil/whs/directives/corres/ins1.html.

Code of Conduct

I

I am an American, fighting in the forces which guard my country and our way of life. I am prepared to give my life in their defense.

II

I will never surrender of my own free will. If in command, I will never surrender the members of my command while they still have the means to resist.

III

If I am captured, I will continue to resist by all means available. I will make every effort to escape and aid others to escape. I will accept neither parole nor special favors from the enemy.

IV

If I become a *prisoner of war*, I will keep faith with my fellow prisoners. I will give no information nor take part in any action which might be harmful to my comrades. If I am senior, I will take command. If not I will obey the lawful orders of those appointed over me and will back them up in every way.

the United States Armed Forces on how to conduct themselves should they become POWs.

The Code provides a clear understanding of the expectations the United States has of its captured service members during periods of conflict.[50] While any service member can be broken through the use of physical and mental torture, the Code seeks to minimize the amount of information that service members give to their captors.[51] The Code takes into account the legal requirements imposed upon captured POWs, and teaches reaction measures when enemy governments fail to follow the laws of war.[52] The Code reflects an in-depth study of the experiences of American POWs in Korea and Viet Nam.[53] It seeks to minimize the ability of hostile nations to use American prisoners as propaganda tools and sources of information. The underlying basis of the Code is helpful when analyzing the dangers to which POWs are exposed when private information is available to captors.

In an attempt to determine why so many Americans had succumbed to propaganda efforts as POWs in Korea, researchers identified attitudes and beliefs of POWs prior to capture as the most reliable indicators about how a person would react to interrogation.[54] The researchers found that Soviet interrogators and their Russian predecessors valued the possession of private information.[55] Private information not only gave valuable insight to those attitudes and beliefs, it made their subjects more susceptible to indoctrination or "brainwashing."[56] Soviet interrogators went to great lengths to compile the "life history" of their subjects regardless of whether their subjects were spies, POWs, or merely subversives.[57]

V

When questioned, should I become a prisoner of war, I am required to give name, rank, service number, and date of birth. I will evade answering further questions to the utmost of my ability, I will make no oral or written statements disloyal to my country and its allies or harmful to their cause.

VI

I will never forget that I am an American, fighting for freedom, responsible for my actions, and dedicated to the principles which made my country free. I will trust in my God and in the United States of America.

Id.

[50] *Id.*

[51] *Id.*

[52] *Id.*

[53] STUART I. ROCHESTER & FREDERICK KILEY, HONOR BOUND; THE HISTORY OF AMERICAN PRISONERS OF WAR IN SOUTHEAST ASIA, 1961-1973 164-65 (1998).

[54] Lawrence E. Hinkle, Jr. & Harold G. Wolff, *Communist Interrogation and Indoctrination of "Enemies of the States;" Analysis of Methods used by the Communist State Police (A Special Report)*, 76 A.M.A. ARCHIVES OF NEUROLOGY AND PSYCHIATRY 139-42 (1956).

[55] *Id.* at 133.

[56] *Id.* at 116, 133.

[57] *Id.* at 133.

Through early and seemingly irrelevant conversation and questioning, an interrogator developed a comprehensive picture of the type of person they were dealing with, their weaknesses, and how those weaknesses could be exploited.[58] A skilled interrogator could bring virtually any prisoner to confess to crimes that he had not committed, and in some cases even cause the prisoner to believe that he was actually guilty of those crimes.[59]

POWs are even more susceptible to interrogation methods because they are often alone and completely at the mercy of their foreign captors.[60] A German interrogator claimed to have elicited nearly all of the information he sought from downed American aircrews during World War II without resorting to physical torture.[61] Upon being taken captive, POWs face several periods of heightened risk. The first period is immediately upon capture because POWs suddenly find themselves in foreign surroundings and needing to rely on their captors' good will for survival.[62] Another period of high risk is when POWs realize the consequences of their capture. For example, the prisoner may spend years awaiting release and have no control over the future.[63] Finally, a third period of high risk occurs when fellow POWs are tortured or threatened with torture.[64]

The method of capture, whether a prisoner is taken alone or as part of a group, also determines initial vulnerability.[65] Captives that are captured alone are more vulnerable as a result of having been cut off from all physical and psychological support.[66] The captive experiences a period of questioning, "why me?" and searches for meaning in the captivity.[67] Almost immediately after capture, POWs begin to realize the consequences of their captivity. Prisoners realize that they may be kept for months or years. Personal freedom has been lost. The captive has no control and is completely dependent upon the captors for support. Children will grow up without a parent. Parents will grow old without their child. Spouses may spend years apart.

---

[58] *Id.*

[59] *Id.* at 137-39.

[60] David K. Kentsmith, *Hostages and Other Prisoners of War*, 147 MIL. MED. 969-70 (1982).

[61] PAT REID, PRISONER OF WAR 71(1984).

[62] Kentsmith, *supra* note 60, at 969.

[63] *Id.* at 969-70.

[64] *See* Robert J. Ursano et al., *The Prisoner of War: Stress, Illness and Resiliency*, 17 PSYCHIATRIC ANNALS 532 (1987).

[65] Ellen Sherwood, *The Power Relationship Between Captor and Captive*, 16 PSYCHIATRIC ANNALS 653, 654 (1986).

[66] *See id.* at 654.

[67] Kentsmith, *supra* note 60, at 969.

Later in captivity, POWs form strong bonds with fellow captives in order to create a support structure.[68] POWs at this stage may be willing to accept torture or even death for themselves, but are unwilling to accept the same consequences for fellow captives. The loss of life control, separation, threats and acts of violence combined with regular contemplation of death and meaning in captivity presents an environment that can cause highly destructive and permanent psychological damage.[69] The psychological breakdown of the individual may then result in information disclosure.

No studies have been conducted about the impact to POWs when faced with hostile acts upon their families. Until the advent of modern technology, it was not a reasonably conceivable threat worthy of significant attention. However, in modern times, POWs who reveal their social security numbers are also revealing the address where their families reside, the identity of their family members, their private financial information, and a great deal of other information that could easily be used to break down the psychological strength of a POW with even the strongest of attitudes and beliefs.

IV. SOCIAL SECURITY NUMBERS AND THE INTERNET: A BAD COMBINATION

Begin with the premise that your social security number has become your national identification number. Use the number to browse selected Internet sites in the business of providing private information, and the result may be disturbing. Networked databases provide a vehicle to consolidate disparate sources of information for relatively easy access by virtually anyone wanting to use it. The final result of data consolidation by networking is a personal profile. A name and social security number can provide an accurate and thorough subject profile that includes financial information,[70] driving history,[71] medical records,[72] public records that

---

[68] Robert J. Naughton, *Motivational Factors of American Prisoners of War Held by the Democratic Republic of Vietnam,* NAVAL WAR C. REV., Jan.-Feb. 1975, at 8-9.

[69] Hinkle & Wolff, *supra* note 54, at 139.

[70] Swire, *supra* note 13, at 464-69 (noting a remarkable trend of private banking and financial institutions maintaining databases with detailed and traceable financial transactions).

[71] 49 U.S.C. § 30302 (establishing the National Driver Register, tracking suspended or revoked licenses, as well as individuals committing serious traffic violations); *see also* Nat'l Highway Traffic Safety Admin., National Driver Registrer, *at* http://www.nhtsa.dot.gov/people/perform/driver (last visited Feb. 2, 2003).

[72] William H. Minor, *Identity Cards and Databases in Health Care: The Need for Federal Privacy Protections*, 28 COLUM. J.L. & SOC. PROBS. 254, 279-81 (1995).

identify number of children, marriage, birth and death certificates,[73] a physical description,[74] a listing of neighbors and associates,[75] political affiliation, business and social networks, buying behavior[76] and even sexual preference.[77] The information is available simply by gathering credit card data, real estate ownership records, voter registration data, auto registration records, marriage records, telephone calling electronic data, web surfing patterns, and other information available electronically and in public records.[78]

The increased availability of private information created the database industry. As the information age grew, so did the fascination with keyboards and mouses, e-commerce and Internet browsing. Every time an individual gets online, the database industry has a feeding frenzy on the data being transmitted, resulting in the development of databases for sale to anyone willing to pay a nominal price. Typically, the information is purchased for only a few cents per name.[79] Conceivably, hostile foreign governments posing as private individuals or businesses attempting to compile profiles or group lists of military members, government employees and contractors could even purchase the information. There is currently no regulatory framework to prevent the exchange of this type of information, nor is there any accurate and meaningful way to trace someone attempting to compile such information.

Private information obtained from the Internet may be used subsequently to conduct surveillance, or threaten to or, even, harm national security personnel, including military members and their families. Conceivably, phone numbers and addresses easily obtained from the Internet could be used to locate personnel for terrorist activity. Medical informa-

---

[73] *See, e.g.,* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1173 (1997) (noting that, traditionally, states view birth, marriage and death certificates as public information).

[74] *See, e.g.,* Domingo R. Tan, Comment, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and the European Union*, 21 LOY. L.A. INT'L & COMP L.J. 661, 661 n.2 (1999) (a private company was enlisted by the federal government to collect photographs from state motor vehicle agencies to develop a national identification database). In the experience of the authors, pictures of military members are also commonly placed in local newspapers to inform friends and family of military achievements.

[75] Jeff Sovern, *Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information*, 74 WASH L. REV. 1033, 1033-1034 & n.2 (1999).

[76] *See generally* Leslie A. Kurtz, *The Invisible Becomes Manifest: Information Privacy in a Digital Age*, 38 WASHBURN L.J. 151, 165-66 (1998).

[77] Sovern, *supra* note 75, at 1034.

[78] Joel R. Reidenberg, *Privacy in the Information Economy: A Fortress or Frontier for Individual Rights?,* 44 FED. COMM. L.J. 195, 197-98 (1992).

[79] ARTHUR M. HUGHES, THE COMPLETE DATABASE MARKETER: SECOND-GENERATION STRATEGIES AND TECHNIQUES FOR TAPPING THE POWER OF YOUR CUSTOMER DATABASE 365 (Rev. ed. 1996).

tion, Internet browsing patterns, purchasing habits, sexual preferences and financial history obtained from the Internet could be used to effectively intimidate and embarrass a service member in POW status. Even worse, the ability of a hostile government to locate a POW's family from information provided by the Internet places the POW in an almost certain position of compromising national security information.

The Internet is an extremely powerful information access tool that requires close observation to prevent it from becoming a weapon for enemy interrogation or to develop intelligence and surveillance information on government personnel responsible for the operation and defense of the United States. When data collection is targeted, profiled and grouped, disclosure to the wrong user can compromise everything from current military operations and defense systems to new defense technology in development. The consequences of allowing the free flow of private information across the global Internet are potentially catastrophic.

When logging onto the Internet using a standard Internet service provider (ISP), users are required to "accept" or "decline" the terms of privacy offered by the ISP. What most users may not be aware of is that accepting the terms of privacy gives the ISP access to the private information provided to them for subscription. This information may include frequency and duration of use, scope of use, credit card numbers, banking information, social security numbers and other identifying and private information. This information then may be transferred or sold to data collection companies or data brokers. Data brokers who consolidate and organize information into a useful data profile for distribution generally supply the demand for private information in the market place. For example, credit card companies with extensive cardholder accounts may maintain data about their cardholders in bulk. A company also may obtain additional bulk data for marketing to potential applicants for credit. The data can even be organized to target specific groups of individuals to meet particular marketing objectives.

Banks, credit bureaus, insurance companies and other commercial institutions sell and trade social security numbers and other private information with little legal limitation. This information could be brokered to a hostile government or organization for intelligence use with the same ease and efficiency it is transferred from Citibank to State Farm Insurance. Companies like Bank of America, who provide travel credit card services to the Department of Defense, and the Uniformed Services Automobile Association Insurance, whose client base is almost exclusively composed of military members and their families, maintain a vast amount of private information. Although self-regulation by private industry is the status quo, there is no obvious control to indicate the effort is anything but a failure. A survey conducted by the Federal Trade Commission (FTC) of 1,400 American companies with Internet sites

revealed that a mere 2% adopted a privacy policy consistent with what the FTC advocates.[80]

The database industry is comprised of approximately 550 firms with annual revenues in the billions of dollars.[81] The average person can be found on about 100 mailing lists and located on fifty or more databases.[82] The availability and collection of private information is so extensive, numerous firms dedicate their business exclusively to data collection. For example, Donnelly Marketing Information Services has a database of at least 125 million people.[83] Wiland Services has a database of 215 million people containing over 1000 elements of information, including demographics and behavioral data.[84] There are an estimated six information collection companies with databases containing data on nearly every household in the United States.[85] Specifically, Axiom Corporation in Conway, Arkansas, has a database combining public and consumer information that covers 95% of American households.[86] In September 1996, LEXIS-NEXIS was selling private information to the public, including personal consumer information, social security numbers, telephone numbers and addresses.[87] LEXIS-NEXIS later permitted individuals to request the removal of their names from the database after the company was subject to a remarkable amount of criticism.[88] In an effort to mitigate damage to their reputation, LEXIS-NEXIS argued that other companies were selling the same information and that it was available publicly.[89] In 1999, Intel and Microsoft both encountered substantial criticism when their customers discovered the memory chips and software in their personal computers transmitted unique identification numbers whenever an individual was using the Internet, thereby providing the ability to interact with other databases.[90] Later in the year, a New Hamp-

---

[80] *The End of Privacy: The Surveillance Society*, THE ECONOMIST, May 1-7, 1999, at 21 [hereinafter *The Surveillance Society*].

[81] Gindin, *supra* note 73, at 1162.

[82] ANNE WELLS BRANSCOMB, WHO OWNS INFORMATION? FROM PRIVACY TO PUBLIC ACCESS 11 (1994).

[83] ERIK LARSON, THE NAKED CONSUMER: HOW OUR PRIVATE LIVES BECOME PUBLIC COMMODITIES 60 (1992).

[84] *Id.*

[85] HUGHES, *supra* note 79, at 354.

[86] *The Surveillance Society*, *supra* note 80, at 21.

[87] Elizabeth Corcoran & John Schwartz, *On-Line Databases Draw Privacy Protests: Unfounded Lexis-Nexis Report Reflects Worry About Growing Files*, WASH. POST, Sept. 20, 1996, at A1; Bruce Haring, *Internet Users Say Data Firm Violates Privacy*, USA TODAY, Sept. 20, 1996, at 3A.

[88] *See* Thomas E. Weber, *Lexis-Nexis Database Sparks Outcry on the Internet About Privacy Issues*, WALL ST. J., Sept. 19, 1996, at B7.

[89] Amy Harmon, *Public Outrage Hits Firm Selling Personal Data*, L.A. TIMES, Sept. 19, 1996, at A1.

[90] *The Surveillance Society*, *supra* note 80, at 22.

shire on-line identification firm called Image Data received financial and technical assistance from the U.S. Secret Service to build a database of driver's license photographs. The company purchased photographs of over 22 million drivers from South Carolina, Florida and Colorado departments of motor vehicles.[91] Image Data argued that the system was used to combat check and credit fraud, but 14,000 e-mail complaints from angry citizens resulted in all three states canceling the sale of the photographs.[92] The disrespect for private information by industry has become pervasive to a point of arrogance. Scott McNealy, Chairman and Chief Executive of Sun Microsystems stated to the media, "[y]ou already have zero privacy—get over it."[93] The news conference was assembled to introduce new software called Jini, designed to interconnect various types of electronic devices.[94]

Prior to mainframe databases and internet servers, the Federal government and most individuals could feel comfortable that their identity and private information would be lost in the obscurity of a massive world population. Obtaining identifying and private information pertaining to any one individual would have required the effort and expense of locating and retrieving hard-copy documents closed away in file cabinets in local, state and federal government offices across America. The collection effort to create an individual profile would have been tedious, time consuming and expensive. Now, mainframes and the vast availability of computers and the Internet have made the same information available at the press of a keyboard button.[95]

The judiciary has recognized the concern for personal privacy.[96] The U.S. Supreme Court expressed its concern of the evolution of information technology, noting that information can be obtained with such efficiency that it robs people of their relative obscurity.[97] The advancement

---

[91] *Id.*

[92] *Id.*

[93] John Markoff, *Growing Compatibility Issue: Computers and User Privacy*, N.Y. TIMES, Mar. 3, 1999, at A1.

[94] *Id.*

[95] *See* Matthew D. Bunker et al., *Access to Government-Held Information in the Computer Age: Applying Legal Doctrine to Emerging Technology*, 20 FLA. ST. U. L. REV. 543, 581-82 (1993).

[96] U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 765 (1989) (recognizing the collection of private information affects privacy more than the danger posed by pieces of information considered separately); Greidinger v. Davis, 988 F.2d 1344, 1353 (4th Cir. 1993); Aronson v. Internal Revenue Service, 767 F. Supp. 378, 388 (D. Mass. 1991) (denying a request for taxpayers' social security numbers under the Freedom of Information Act because it reveals private information about individuals); State ex rel. Beacon Journal Publishing Co. v. City of Akron, 640 N.E.2d 164, 169 (Ohio 1994) (recognizing ease of obtaining personal information).

[97] *See Reporters Comm.*, 489 U.S. at 780.

each year of computer and information technology is exponential, and searches for private information become easier and less costly while the threat to privacy is dramatically increased. As the problem goes ignored, the threat to America's national security becomes an even greater issue. For many years, the losing battle for privacy on the Internet was addressed almost exclusively with constitutional arguments.[98] However, our justice system must rethink the concept of privacy and factor national security into the Internet privacy question, especially as it pertains to military and other government personnel associated with national security. The Internet is a growing source of intelligence for hostile governments and organizations. Failure to appropriately address this threat would be nothing less than naïve and careless.

V. INADEQUATE LEGAL PROTECTION FOR PRIVATE INFORMATION

A. *Protection of Private Information Under the Freedom of Information Act*

The Freedom of Information Act (FOIA) was passed in 1988 in an effort to provide full disclosure of information in the possession of Federal agencies.[99] American citizens have an inherent role in reviewing the activities of the U.S. government and its representatives to ensure accountability. Access to official records and documents produced by the government provides insight into the workings of the government and gives the public a better ability to scrutinize its activities. FOIA requires Federal agencies to make records available to the public unless a specific statutory exemption applies.[100] FOIA contains several critical exemptions designed to prevent the disclosure of private information[101] and to preserve sensitive government records.[102] The exemptions allow agencies to withhold information related to national security, personnel, medical and similar files, when disclosure would be invasive to personal privacy.[103]

---

[98] *See supra* note 12 for case references regarding constitutional protection of privacy.

[99] S. REP. NO. 89-813, at 2-3 (1965).

[100] 5 U.S.C. § 552(a)(3) (1994).

[101] *See, e.g., id.* § 552(b)(6) (1994).

[102] *Id.* § 552(b)(1)(A) (1994). *See also* H.R. REP. NO. 89-1497, at 3-4 (1966); S. REP. NO. 89-813, at 3 (1965).

[103] *Id.* § 552(b)(6). Records not specifically exempt under FOIA must promptly be made available to any person. *Id.* § 552(a)(3). Moreover, FOIA requires federal agencies to state their reasons for withholding documents. *Id.* § 552(a)(6)(A)(i); *see also id.* § 552(b)(1)-(9). The remaining FOIA exemptions include documents relevant to: 1) agency rules and practices; 2) confidential business information; 3) interagency or intra-agency memoranda; 4) law enforcement investigations; 5) banking reports; and 6) information about oil and gas wells. *Id.* § 522(b).

The most important FOIA exemption for purposes of this discussion is Exemption Six, allowing an agency to withhold records that would "disclose information of a personal nature where disclosure would constitute a clearly unwarranted invasion of personal privacy."[104] This is a particularly valuable premise for military members and other government personnel working in national security roles.[105] In light of this exemption, the judiciary has consistently determined that an individual's social security number is not releasable under the FOIA.[106] These decisions reflect judicial awareness of the sensitivity toward the Federal government's dissemination of social security numbers. The FOIA provides no protection from the dissemination of private information by commercial industry. Moreover, contrary to the spirit of privacy illustrated in FOIA Exemption Six, the Department of Defense effectively requires disclosure of a POW's social security number to enemy forces in order to comply with the GPW.

B. *Protection of Private Information Under the Administrative Procedures Act*

The Administrative Procedure Act (APA) of 1946[107] recognizes that official records and documents are subject to public access much like they are under FOIA.[108] The executive branch, however, is also granted broad discretion through government agencies to determine what information should be exempt from disclosure "in the interest of national defense or foreign policy."[109] A determination is also made as to whether the requester has a valid reason for obtaining information.[110] Based on these premises, Federal agencies use the APA to preclude disclosure of information to the public.[111]

Congress and federal agencies have recognized the importance of protecting social security numbers and other private information from distri-

---

[104] *Id.* § 552(a)-(b) (1994).

[105] *Id.* § 1002 (1946).

[106] *See, e.g.*, Sheet Metal Workers Int'l Assn., Local No. 9 v. United States Air Force, 63 F.3d 994 (10th Cir. 1995); Painting Ind. of Hawaii Market Recovery Fund v. United States Dep't of Air Force, 26 F.3d 1479 (9th Cir. 1994); Int'l Bhd. of Elec. Workers Local Union No. 5 v. Dep't of Hous. & Urban Dev., 852 F.2d 87 (3d Cir. 1988); Aronson v. Internal Revenue Service, 973 F.2d 962, 968 (1st Cir. 1992); Heights Cmty. Cong. v. Veterans Admin., 732 F.2d 526 (6th Cir. 1984).

[107] 5 U.S.C. § 1002 (1946).

[108] *Id.*

[109] 5 U.S.C.S. § 552(a)(1)(A) (1994).

[110] *Id.*

[111] Steven Helle, *The News-Gathering/Publication Dichotomy and Government Expression*, 1982 DUKE L.J. 1, 58-59 (1982); Paul A. Ruben, Note, *Applying the Freedom of Information Act's Privacy Exemption to Requests for Lists of Names and Addresses*, 58 FORDHAM L. REV. 1033, 1035 (1990); Bunker et al., *supra* note 95, at 553-55.

bution by the federal government, but have largely failed to address the distribution of the same information by private industry or through the Department of Defense. Data collection businesses and brokers of private information cannot be charged with violating the APA. The APA provides statutory rights only against the government. There is essentially no legal recourse against a private business or individual collecting or distributing private information, especially on the international level.[112] Further, there is no legal recourse against a hostile government or organization collecting information for potential harm to federal government personnel.

C. *Protection of Private Information Under the Privacy Act*

In response to the growing threat computer technology has on individual privacy, Congress passed the Privacy Act of 1974[113] to "promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government."[114] Although the Privacy Act is protective to the extent that it precludes the disclosure of private information without an individual's consent, it also provides an individual access to all information collected by the federal government.[115] The Privacy Act provides the right of access to personal records and the opportunity to correct records based on a showing of error, relevancy, timeliness or completion.[116] The Privacy Act does not apply to selected law enforcement and national security agencies like the Federal Bureau of Investigation, the Central Intelligence Agency or the Secret Service.[117]

The Privacy Act recognizes that an individual's privacy is directly affected by the federal government's ability to collect, maintain and use the information. Further, the use of computers and information management systems has escalated the potential for harm. Further, the Privacy Act recognizes that the right to privacy is a personal and fundamental right protected by the Constitution, and that Congress is entrusted with the powers and responsibility to protect that right. A fundamental prob-

---

[112] *See, e.g.*, United States v. McAllister, 18 F.3d 1412, 1417-18 (7th Cir. 1994); United States v. Reed, 15 F.3d 928, 931 (9th Cir. 1994); Pleasant v. Lovell, 974 F.2d 1222, 1226 (10th Cir. 1992); United States v. Attson, 900 F.2d 1427, 1432 (9th Cir. 1990).

[113] H.R. REP. NO. 93-1416, at 7 (1974); 5 U.S.C. §552a (1994).

[114] S. REP. NO. 93-1183, at 1 (1974).

[115] 5 U.S.C. §552a(b)-(d). Individuals may request that inaccurate records be corrected by the holding government agency. *Id.* §552a(d)(2). If the request is denied, civil action may be exercised and the agency may be ordered to correct the inaccurate information. *Id.* §552a(d)(3).

[116] *Id.* § 522a(d)(2)(B)(i).

[117] *Id.* § 552a(j)(1)-(2), (k)(3).

lem with the Privacy Act is that it was created when government records were stored almost entirely in hard-copy format. Although the Privacy Act recognizes the importance of preserving the right to privacy, the boundless ability to store data that currently exists renders the Act a lame law absent further posturing by Congress.[118]

In the United States, a person's social security number has become a universal personal identification number.[119] Congressional committees expressed concern over this possibility while considering whether to adopt the Privacy Act. In one supporting report, a Senate Committee commented that use of the social security number as a personal identification number is "one of the most serious manifestations of privacy concerns in the nation."[120] Section 7 of the Privacy Act dictates that the federal government cannot require an individual to provide a social security number unless specific permission was granted from Congress to require release.[121] Similar to the protective provisions of FOIA, Section 7 seems to provide a significant measure of protection. However, the exception allowing Congress to require release of a social security number is problematic.

Congress granted the Department of Defense authority to require use of social security numbers in place of registration numbers in 1969,[122] thus requiring military members to provide their social security numbers to enemy forces upon apprehension as POWs.[123] The exception to Sec-

---

[118] Bunker et al., *supra* note 95, at 583-84 (*citing* FLORIDA JT. LEGIS. INFO. TECH RESOURCE COMM., FLORIDA'S INFORMATION POLICY: PROBLEMS AND ISSUES IN THE INFORMATION AGE 28 (1989) and Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(4), 88 Stat. 1897 (1974). *See also* H.R. REP. NO. 93-1416, at 9 (1974).

[119] *See* DAVID H. FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 78 (1989). *See also* Minor, *supra* note 72, at 261-71.

[120] S. REP. NO. 93-1183 (1974), *reprinted in* 1974 U.S.C.C.A.N. 6916, 6943.

[121] *See* Pub. L. No. 93-579, § 7. This provision of the Privacy Act was never codified, but is instead set out as a historical note to 5 U.S.C.A §552a (West 1996). The full text states the following:

> (1) It shall be unlawful for any Federal, State, or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number. (2) The provisions of paragraph (1) of this subsection shall not apply with respect to (A) any disclosure which is required by Federal statute, or (B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. (b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall 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.

Id. §7.

[122] *History of Chronology, supra* note 16.

[123] *See* GPW *supra* note 25, art. 17

tion 7 makes the social security number exemption useless for military members trying to protect their private information. Congress and the Department of Defense have placed military members in the awkward position of having to provide their name, rank, service and social security number to enemy captors, enough information to compromise the military member in an interrogation. However, the requirement is ironically inconsistent with Congressional and judicially recognized public policy to protect social security numbers as private information.

D. *The Failure of the Existing Framework of Privacy Laws*

Although not specifically provided in the U.S. Constitution, the Supreme Court has fashioned a doctrine of privacy protection through constitutional amendments, including the First Amendment's freedom of expression and association;[124] the Fourth Amendment's protection of persons, places, papers and effects;[125] the Fifth Amendment's privilege against self-incrimination;[126] and the protection of liberty found in the Ninth and Fourteenth Amendments.[127] The right of an individual to be secure in their person, house, papers and effects against unreasonable searches and seizures should be extended beyond protection from the government, but also from private industry, private organizations, private citizens, foreign governments and military forces.

Some authors espouse the philosophy that individuals have ownership of their private information much like intellectual property, and the rights to that information are derived from the law of trademark, copyright and publicity.[128] Moreover, if the information is bought and sold, the initial purchase of the information should be directly from the individual who owns the information.[129] Further commercial sale, use or transfer of the information would require consent and royalties.[130] These arguments for ownership of private information need to be balanced against the First Amendment freedom of the press.[131]Although creative, the advancement of privacy protection to this level limits the media's already arguable abil-

---

[124] Stanley v. Georgia, 394 U.S. 557, 564-66 (1969); NAACP v. Alabama ex rel. Patterson, 357 U.S. 449, 460-63 (1958).

[125] Katz v. United States, 389 U.S. 347, 350-53 (1969) (establishing protection of persons under the Fourth Amendment); Olmstead v. United States, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting); Boyd v. United States, 116 U.S. 616, 627-30 (1886).

[126] Mapp v. Ohio, 367 U.S. 643, 656-57 (1961) (noting that an unconstitutional seizure is tantamount to coerced self-incrimination).

[127] Griswold v. Connecticut, 381 U.S. 479, 484-85 (1965); Roe v. Wade, 410 U.S. 113, 152-53 (1973).

[128] Ann Bartow, *Our Data, Ourselves: Privacy, Propertization, and Gender,* 34 U.S.F. L. REV. 633, 687-99 (2000).

[129] *Id.* at 687.

[130] *Id.*

[131] For a discussion of First Amendment freedom of the press provisions balanced against the privacy interests of an individual see Florida Star v. B.J.F., 491 U.S. 524

ity to investigate news stories since there would be no access to private information without cost or consent. Private information is needed to accurately investigate and report stories to the public. Under the broad cover of constitutional protection, the media is largely a profit motivated industry that does not regulate itself and is already challenged in the delivery of information to the public. Further limitation would compound this concern. Requiring consent or payment for information further limits the media's ability to responsibly report information, and arguably limits free speech.

Data collection businesses and brokers of private information cannot be charged with violating the FOIA, the APA, the Privacy Act or traditional rights to privacy protected by the Constitution. The traditional vehicles for protection of privacy set forth rights against the government only. There is essentially no legal recourse against a private business or individual collecting or distributing private information, especially on the international level.[132]

VI. THE EUROPEAN MODEL AND PROPOSED U.S. LEGISLATION: THE WAY AHEAD?

A. *The European Union Data Protection Directive*

The European Union Data Protection Directive (EUDPD)[133] is an attempt to control the commercial exploitation of private information by informing individuals what their private information is being used for and to whom it is being given. The EUDPD applies to both electronic and paper filing systems.[134] The directive covers material containing identifying information such as an individual's name or identification number. Private information is termed "Personal Data" in the EUDPD, meaning any information relating to an identified person, the "data subject." An identifiable person is one who can be identified, directly or indirectly, by reference to an identification number or other data that may include physical, physiological, mental, economic, cultural or social identity.[135]

In recognition of basic privacy, the EUDPD directs that private information should only be collected for specific, legitimate reasons.[136] Further, the information cannot be kept any longer than necessary to fulfill

---

(1989) striking down an award of compensatory and punitive damages against a newspaper which published the name of a rape victim in violation of a Florida statute.

[132] *See, e.g.*, United States v. McAllister, 18 F.3d 1412, 1417-18 (7th Cir. 1994); United States v. Reed, 15 F.3d 928, 931 (9th Cir. 1994); Pleasant v. Lovell, 974 F.2d 1222, 1226 (10th Cir. 1992); United States v. Attson, 900 F.2d 1427, 1432 (9th Cir. 1990).

[133] Council Directive 95/46/EC, arts. 11, 12, 14, 1995 O.J. (L 281) 31 [hereinafter European Community Directive on Data Protection].

[134] *Id.* art. 3, at 39.

[135] *Id.* art. 2, at 38.

[136] *Id.* ch. II, art. 6(b), (d), (e), at 40.

the purpose of collection.[137] Whoever is collecting the information must give notice to the data subject and explain why the information is being collected, who is collecting it and who will have access.[138] If there is any error in the data, the data subject may access the information and make any necessary corrections.[139] The EUDPD requires a data subject to give explicit consent prior to collection and access to sensitive information associated with race, ethnicity, religion, political affiliation, philosophical beliefs, memberships, sexual preference and health.[140]

The EUDPD is premised on the principal that an individual possesses a fundamental right to protect private information. Moreover, it is an attempt to protect European Union citizens from the aggressive wave of data collection and distribution similar to that in the United States.[141] In sharp contrast, the United States has no meaningful and comprehensive law similar to the EUPDP that protects private information.[142] The failure of Congress to adequately respond to the privacy protection crisis questions whether the political emphasis is on protection of commerce and big business over national security and an individual's right to protect private information.[143] Remarkably, the current state of existing infor-

---

[137] *Id.* ch. II, IV, at 41-42.

[138] *Id.* ch. II, IV, art. 10, at 41.

[139] *Id.* ch. II, IV, art. 10(c), at 41.

[140] *Id.* ch. II, III, arts. 8(1), 8(2)(a), at 40.

[141] PETER P. SWIRE & ROBERT E. LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTORNIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE 3 (1998).

[142] *See, e.g.*, Denise Caruso, *Exploiting - and Protecting - Personal Information*, N.Y. TIMES, Mar. 1, 1999, *at* http://www.nytimes.com/library/tech/99/03/biztech/articles/01digi.html. The Clinton administration advocated the interest of the data broker industry, stating that "U.S. companies should not be forced to give people access to personal information about themselves." Jeri Clausing, *Administration Seeks Input on Privacy Policy*, N.Y. TIMES, Nov. 6, 1998, *at* http://www.nytimes.com/library/tech/98/11/cyber/articles/06privacy.html. Perhaps most telling of the importance of the protection of private information, the Clinton administration failed to support a Federal Trade Commission proposal for legislation on internet consumer privacy. *See* Stephen Labaton, *White House and Agency Split on Internet Privacy*, N.Y. TIMES, May 23, 2000, *at* http://www.nytimes.com/library/tech/00/05/biztech/articles/23privacy.html. Labaton reported that:

> Clinton administration officials today threw cold water on a proposal by the Federal Trade Commission for legislation to protect consumer privacy on the Internet. . . . Administration officials were decidedly lukewarm [to the FTC proposal]. They said that the government should continue to rely on the industry to police itself and that the White House had a deeper interest in promoting privacy laws in other areas.

Id.

[143] The divergent views of Americans and Europeans has been studied, providing some possible explanations for the differences. Although Europeans see the protection of personal data as a fundamental human right, Americans may have more

mation law suggests Congress is more alarmed by the federal government's ability to collect and distribute private information than it is about the real danger–private industry and the international community. Congress appears to have more trust and confidence that data collection companies and brokers will protect private information and national security than it trusts itself to do the same. For example, Congress has promulgated statutory restrictions on the law enforcement community's collection of information associated with items as important as driver licenses,[144] medical records,[145] credit reports[146] and phone records,[147] to information as obscure as cable subscription information[148] and video rental records.[149] These laws place restrictions only on government. In a recent report to Congress on the state of Internet privacy, the FTC encouraged protection of consumer privacy and private information.[150] Even before the September 11th attacks, Americans were alarmed by the inadequate protection of their privacy on the Internet.[151] Fifty-seven percent of Americans expressed a desire for Congress to pass legislation similar to the EUDPD, providing protections of the use of private information on the Internet.[152]

The adoption of the EUDPD has had little impact on the German military.[153] The primary reason being that the German military uses a unique identification code for the purposes of the Geneva Convention Relative to the Treatment of Prisoners of War.[154] The code requires the service

---

trust in private industry, placing confidence in the media to expose abuses. Americans are also hesitant to develop more regulation of information exchange at the expense of First Amendment rights. *See* Pamela Samuelson, *A New Kind of Privacy? Regulating Uses of Personal Data in the Global Information Economy*, 87 CAL. L. REV. 751, 756-57 (1999) (*reviewing* PAUL M. SCHWARTZ & JOEL R. REIDENBERG, DATA PRIVACY LAW: A STUDY OF UNITED STATES DATA PROTECTION (1996); SWIRE & LATIN, *supra* note 141.

144 *See* 18 U.S.C. § 2721 (1994) (prohibiting the disclosure of private information by state motor vehicle registration agencies without the consent of the registrant).

145 *See* Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 1320a-7e (2000); *see also* Statement on Signing the Health Insurance Portability and Accountability Act of 1996 [Health Insurance Portability and Accountability Act], 32 Weekly Comp. Pres. Doc. 1480 (Aug. 26, 1996).

146 *See* Fair Credit Reporting Act, 15 U.S.C. § 1681 (1994).

147 *See* 18 U.S.C §§ 2510-2522, 3121 (1994).

148 *See* Cable Communications Policy Act of 1984, 47 U.S.C. § 551 (1994).

149 *See* Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (1994).

150 Sen. Ernest F. Hollings, *Individual Privacy on the Internet*, PRIVACY NEWSLETTER (Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, PC), Aug. 2001, at 1.

151 *Id.*

152 *Id.*

153 E-mail from former German Air Force Captain, Joerg Gerhardus, January 20, 2003 (on file with authors). Mr. Gerhardus has recently immigrated to the United States and works in consumer protection.

154 *Id.*

member's date of birth and first initial of the last name, then a series of numbers and letters unique to the individual.[155] Knowing a German service member's serial number does not result in access to other data because the serial number is used solely for military purposes. Because the German government uses several identification codes for unique purposes, identity theft or data collection through the possession of one single number is limited in scope. The drawback is that remembering all of these numbers can be difficult, but identity theft in Germany is much more rare, and much more limited in scope.[156]

B. *Senate Bill 2201*

In response to the demand for private information protection, the U.S. Senate is in the process of developing privacy legislation for the Internet called the On-line Personal Privacy Act (On-line Privacy Act).[157] Introduced by Sen. Ernest F. Hollings, the most important sections of the On-line Privacy Act require commercial Internet companies to obtain consent before collecting or using an individual's private information.[158]

---

[155] *Id.*

[156] *Id.*

[157] *See* S. Res. 2201, 107th Cong. (2002).

[158] *Id.* Section 106 of the proposal says: "An Internet service provider, online service provider, or operator of a commercial website shall establish and maintain reasonable procedures necessary to protect the security, confidentiality, and integrity of personally identifiable information maintained by that provider or operator." Section 401 provides several key definitions. For example, "personally identifiable information" is:

> [i]ndividually identifiable information about an individual collected online, including—(i) a first and last name, whether given at birth or adoption, assumed, or legally changed; (ii) a home or other physical address including street name and name of a city or town; (iii) an e-mail address; (iv) a telephone number; (v) a birth certificate number; (vi) any other identifier for which the Commission finds there is a substantial likelihood that the identifier would permit the physical or online contacting of a specific individual; or (vii) information that an Internet service provider, online service provider, or operator of a commercial website collects and combines with an identifier described in clauses (i) through (vi) of this subparagraph. (B) Inferential information excluded - Information about an individual derived or inferred from data collected online but not actually collected online is not personally identifiable information.
>
> (12) Release - The term "release of personally identifiable information" means the direct or indirect, sharing, selling, renting, or other provision of personally identifiable information of a user of an internet service, online service, or commercial website to any other person other than the user.
>
> (13) Robust notice - The term "robust notice" means actual notice at the point of collection of the personally identifiable information describing briefly and succinctly the intent of the Internet service provider, online service provider, or operator of a commercial website to use or disclose that information for marketing or other purposes.
>
> (14) Sensitive financial information - The term "sensitive financial information" means—(A) the amount of income earned or losses suffered by an individual;

Similar to the EUDPD, the On-line Privacy Act requires Internet companies to give notice of their privacy policies and allows individuals to access the information collected to determine what private information is subject to potential distribution.[159] The proposal also provides legal recourse in the event any private information is misused or released without consent.[160] If an individual allows private information to be disclosed, then an Internet company must have the individual affirmatively "opt-in;" whereas the disclosure of non-private information would invoke an "opt-out" decision.[161] The legislation proposes that the FTC will have both rulemaking and enforcement authorities.[162]

Although the On-line Privacy Act is a welcome first attempt by Congress to embrace the privacy crisis, it fails to fully address the national security threat because it has no application to the international community. Further, it does not protect the disclosure of a social security number as a personal identification number to comply with GPW and Department of Defense requirements. There is no indication the legislation has any applicability to federal agencies. Although the legislation addresses the collection and distribution of private information domestically, the threat of collection and distribution of the same information among foreign governments and organizations remains a significant threat.

VII. CONCLUSION

When the Department of Defense began to use social security numbers in place of registration numbers in 1969, it would have been virtually impossible to comprehend the consequences of how the numbers could be associated with large amounts of private information on the Internet. The development of the social security number as a national identification number for both military and commercial purposes has created both

---

(B) an individual's account number or balance information for a savings, checking, money market, credit card, brokerage, or other financial services account; (C) the access code, security password, or similar mechanism that permits access to an individual's financial services account; (D) an individual's insurance policy information, including the existence, premium, face amount, or coverage limits of an insurance policy held by or for the benefit of an individual; or (E) an individual's outstanding credit card, debt, or loan obligations.

(15) Sensitive personally identifiable information - The term "sensitive personally identifiable information" means personally identifiable information about an individual's—(A) individually identifiable health information (as defined in section 164.501 of title 45, Code of Federal Regulations); (B) race or ethnicity; (C) political party affiliation; (D) religious beliefs; (E) sexual orientation; (F) a Social Security number; or (G) sensitive financial information.

Id. § 401.

[159] *Id.* § 102.

[160] *Id.* § 204-5.

[161] *Id.* § 102.

[162] *Id.* § 201, 403.

a privacy and national security nightmare. The statement is especially true for service members effectively required to provide their social security number to enemy forces while a POW. Arguably, the Department of Defense is subject to suit for requiring disclosure of social security numbers under these conditions because the practice defies the letter, spirit, logic and overall principle of privacy defined by the Constitution and other statutory protections.

The simple and most practical solution is for the federal government, and especially the Department of Defense, to stop using the social security number as a national identification number. Returning to a separate "serial number" system used exclusively for military identification is a basic measure that affords significant protection to service members while continuing to comply with international law. Presumably, a "serial" number could not be associated with any other private information. Further, educating service members on the dangers of disclosing private information to captors, in conjunction with the amount of information available on the Internet, would be equally useful.

Privacy and national security interests merge on the point of abolishing the social security number as a national identifier. Congress has demonstrated a great effort to protect individuals from the collection and access of private information by the federal government, but has no law in place that protects Americans from collection by private industry and foreign governments. If passed, the On-line Privacy Act is a first step towards addressing commercial distribution of private information. However, comprehensive protection must also address collection and distribution of private information by foreign governments. This protection may be achieved through international agreements and restrictive domestic legislation. In the age of the information superhighway and the global war on terrorism, America must focus on the protection of service members and national security. In an effort to find the ultimate solution, artful legislators targeting the national security threat have a unique opportunity to further initiate further protection of personal privacy.