Quentin M. Rhoades
State Bar No. 3969
SULLIVAN, TABARACCI & RHOADES, P.C.
1821 South Avenue West, Third Floor
Missoula, MT 59801
Telephone: (406) 721-9700
Facsimile: (406) 721-5838
qmr@montanalawyer.com

Attorneys for Plaintiff

MONTANA FOURTH JUDICIAL DISTRICT COURT, MISSOULA COUNTY

MONTANA SPORTS SHOOTING ASSOCIATION, INC., GARY S. MARBUT, ROBERT C. CLARK, CAROL LATTA, Plaintiffs, v. **THE STATE OF MONTANA, MIKE MCGRATH, ATTORNEY GENERAL OF THE STATE OF MONTANA, THE MONTANA DEPARTMENT OF FISH, WILDLIFE AND PARKS,** Defendants.	**Cause No. DV-06-94** **Dept. No. 1** ***PLAINTIFFS' MONTANA SHOOTING SPORTS ASSOCIATION, INC. AND GARY S. MARBUT'S ANSWERS TO DEFENDANTS' FIRST DISCOVERY REQUESTS***

COME NOW Plaintiffs, Montana Shooting Sports Association, Inc., and Gary S. Marbut, ("Plaintiffs"), and respond to Defendants' First Discovery Requests to Plaintiffs, dated August 21, 2006, as follows:

INTERROGATORIES

INTERROGATORY NO. 1: Please identify each person or persons preparing Plaintiffs' response to these combined discovery requests by providing each person's name, address and phone number.

ANSWER:

1. Quentin M. Rhoades
1821 South Avenue West, 3rd Floor,
Missoula, Montana 59801
Phone: 406-721-9700

2. Gary Marbut
Montana Sports Shooting Association
P.O. Box 16106
Missoula, Montana 59808
Phone: 406-549-1252

INTERROGATORY NO. 2: Please identify the name, and if known, the address and telephone number of each individual likely to have discoverable information that you may use to support your claims, identifying the subjects of the information.

ANSWER: Unknown at this time. In addition, Plaintiffs continue to diligently search for such information and to the extent such information is discovered in the future, this response will be supplemented.

INTERROGATORY NO. 3: Please identify all documents, data compilations and tangible things that are in your possession, custody or control that you may use to support your claims.

ANSWER: See requests for production. In addition, Plaintiffs continue to diligently search for such documentation in their own records and are seeking such documents from Defendant and other witnesses. To the extent such documents are discovered in future, this response will be supplemented.

INTERROGATORY NO 4: If you object to the production of any of the materials subject to the request for production set forth herein, for each document withheld based upon such objection, please identify the date of (sic) the final version of each document was created; the date of each draft, if any, was created; the author(s) of the document; the recipient(s) of the document, if any; and all of those who received copies of such each (sic) document withheld.

ANSWER: Anything that would breach privacy or be subject to attorney-client privilege. See requests for production.

INTERROGATORY NO. 5: MISSING FROM DEFENDANTS' INITIAL DISCOVERY REQUESTS.

INTERROGATORY NO. 6: For each of the individually named plaintiffs, please set forth each and every instance in the last ten years, with specificity as to the date, type of

instance and purpose of instance, in which you have provided your Social Security Number to obtain employment; receive legislative pay and benefits; buy goods and services; buy a vehicle; participate in a local, state or federal government programs (sic); apply or register for any local, state or federal government license, registration or permit; apply for or maintain a concealed weapon permit; apply for credit; rent or buy a residence; obtain medical care; apply for or use any type of insurance; obtain a driver's license; join a group or association; and any other instance in which you were requested to provide your social Security Number and did so.

ANSWER: Employment; none. Legislative benefits and pay; none. Buy goods and services; none. Buy a vehicle; none. Participate in a government program; none. Apply for government license; see following. Maintain a concealed weapon permit; 01/19/04 - renewal. Renewal of Montana drivers license; 09/24/01.

Apply for credit; none. This item requires further explanation. Within the last ten years, I have applied for numerous credit cards, but have always deliberately not supplied my SSN on the application. I have been granted one credit account notwithstanding the non-provision of the SSN. Since being granted that account, I have not applied for others. In addition, I have a banking relationship with a local bank. I have a business line of credit with that bank that is renewed annually. This bank has had my SSN on file for more than ten years, and I decline to resubmit it for the annual renewal of the line of credit. I have refinanced my home mortgage within the last ten years, but I have not provided my SSN anew for this refinance since the bank has it on file from prior business. This same bank asked me to provide my SSN over the Internet in order to avail myself of its Online banking features. I complained to the bank about this requirement and subsequently declined to participate in Online banking because of the bank's SSN requirement (See Mont. Code Ann. § 32-6-306.) I am told that because of my objection to its Internet Website programming requiring an SSN for registration, the bank has removed the requirement that a customer provide an SSN to register for Online banking.

Rent or buy a residence; none, except above. Obtain medical care; none. Apply for or use any type of insurance; none. Join a group or association; none. Other instances; I provide my SSN to the State of Montana, Department of Revenue, and the Internal Revenue Service annually upon submissions of income tax returns.

INTERROGATORY NO. 7: Please set forth each and every instance in which you allege identity theft as a result of the passage and implementation of MCA 87-2-106 and MCA 87-2-202.

ANSWER: None that I am aware of as of this date, but I am watching for such an occurrence and I will not be surprised if it happens.

INTERROGATORY NO. 8: Please set forth each and every instance in which you allege Defendant Montana Fish, Wildlife and Parks (sic) failed to protect from unauthorized disclosure a Social Security Number gathered in compliance with MCA 87-2-106 and MCA 87-2-202.

ANSWER: See answers to Interrogatories Nos. 12 and 14. The State of Montana and the Montana Department of Fish, Wildlife and Parks (FWP) have inadequate security provisions and policies to assure protection of sensitive personal data. Because all persons handling sensitive personal data, from temporary, privately employed clerks to private and state computer repair and maintenance personnel do not have security clearances and periodic background checks, because all computer traffic associated with handling sensitive personal data may or may not be encrypted according to accepted encryption standards, such as Triple Defense Encryption Standard (3DES) with a minimum 128-bit encryption key, because all private and public facilities where sensitive personal data is stored is not secured according to best accepted practices for physical security, it is impossible to point to specific instances of breach of security (See the newspaper article reference in answer to Interrogatory No 14 about FWP computers being hacked). These shortcomings suggest that every time the State and FWP have collected the required sensitive personal data from a citizen for purchase of a license may well have constituted a failure to properly secure sensitive data.

INTERROGATORY NO. 9: Please set forth each and every instance in which you allege Defendant Montana Fish, Wildlife and Parks (sic) failed to provide adequate safeguards to ensure a Social Security Number gathered in compliance with MCA 87-2-106 and MCA 87-2-202 were (sic) protected from unauthorized disclosure.

ANSWER: See answers to Interrogatories Nos. 12 and 14. The State of Montana and the Montana Department of Fish, Wildlife and Parks (FWP) have inadequate security provisions and policies to assure protection of sensitive personal data. Because all persons handling sensitive personal data, from temporary, privately employed clerks to private and state computer repair and maintenance personnel do not have security clearances and periodic background checks, because all computer traffic associated with handling sensitive personal data may or may not be encrypted according to accepted encryption standards, such as Triple Defense Encryption Standard (3DES) with a minimum 128-bit encryption key, because all private and public facilities where sensitive personal data is stored is not secured according to best accepted practices for physical security, it is impossible to point to specific instances of breach of security. These shortcomings suggest that every time the State and FWP have collected the required sensitive personal data from a citizen for purchase of a license may well have been not adequately protected from unauthorized disclosure.

INTERROGATORY NO. 10: Please state for each individually named (sic) plaintiff whether he or she has provided his or her Social Security Number to obtain a Driver's license, the last year in which the application was made and the state of the application.

ANSWER: See Answer to Interrogatory No. 6.

INTERROGATORY NO. 11: For each individually named (sic) plaintiff, please state whether you or a member of your family has ever received public assistance of used child support enforcement services in the State of Montana.

ANSWER: No, however for anyone with a positive answer to this question, asking the question and demanding an answer would be a violation of the Montana constitutional right to privacy. It is offensive that you ask.

INTERROGATORY NO. 12: Explain why the requirement to provide a Social Security Number on a wildlife conservation license, hunting, fishing, or trapping license is a violation of the right to privacy.

ANSWER: The right to privacy in Montana has been secured from government intrusion by the people of Montana in their Constitution. By placing the right to privacy in the Montana Constitution, the people of Montana have limited the franchise of power to State government - have said "Here the government may not tread." They have placed individual privacy outside the reach of government under its limited charter. It is also worth reiterating the opening declaration by the citizens of Montana when they franchised government with a limited grant of power from the people. They said, "All political power is vested in and derived from the people ..." This gives special meaning to the right of privacy as a strict limitation on the power of government agencies and personnel. The right to privacy in Montana is a fundamental right, and one that by declaration requires a "compelling state interest" to override. Further, the right to privacy is a direct bar to State action. *St. v. Long*, 216 M 65, 700 P2d 153, 42 St. Rep. 643 (1985).

In his 2003 Montana Law Review article, *RESTORING PRIVATE TO PRIVACY*, U. of M. law professor Jeffrey T. Renz discusses the *Long* decision which held that the Montana constitutional right to privacy restrains only state actors.

One point in the article is a quote from the floor session of the 1972 Constitutional Convention, quoting Bob Campbell, a delegate and the author of the right to privacy:

> "[P]olitical organizations, private information gathering firms, and even an individual can now snoop more easily and effectively than ever before. We certainly hope that such snooping is not as widespread as some persons would have us believe, but with technology easily available and becoming more refined all the time, prudent safeguards against the misuse of technology are needed." (5 MONT. CONST. CONV. TR. 1681 (1972))

This points out that the right to privacy in the Montana Constitution is specifically intended to prevent snooping, and under the *Long* decision, especially snooping by the state. Contrarily, the very purpose of SSN use is to make snooping easier -- to enable and empower the state and state actors to easily, quickly and conveniently snoop into the

private lives of private people. Thus, anything that is specifically designed to facilitate government snooping must be in conflict with the declared intent of the right to privacy that the people of Montana have reserved to themselves from government intrusion.

The State will make the argument that it must collect SSNs from hunters and anglers in order to meet the federal condition that it do so to maintain eligibility to receive certain federal funding.

To breach this Montana right in order to obtain money, regardless of amount or source, means that the state sees rights as for sale - that those areas of power reserved from State interference by the people may be sold by the state to the highest bidder at an elaborate government bake sale. There is no doubt that government sale of rights reserved to the people by the people is unacceptable, intolerable and unpardonable. Although what constitutes a "compelling state interest" will be discussed and defined by others, it is easy to say what it is not. A compelling state interest is not the simple acquisition of money, whatever source of funding happens to be available.

Economic issues are not a basis for surrender of constitutional rights. In a case involving newspaper access to Department of Corrections bidding negotiations, the M.C.A. annotations say: "The state contended that the meetings at issue were closed for economic advantage, but economic advantage is neither a privacy interest nor a sufficient reason for denying the public the opportunity to observe deliberations of public bodies or to examine public documents, including proposals submitted to the public body by a vendor, unless the proposal concerns a privacy interest involving legitimate trade secrets or individual safety. A public agency's desire for privacy does not provide an exception to the public's constitutional right to observe its government at work. To the extent that provisions in 18-4-304 or ARM 2.5.602 require exclusion of the public from the competitive bid process, those provisions are unconstitutional and unenforceable. *Great Falls Tribune Co., Inc. v. Day*, 1998 MT 133, 289 M 155, 959 P2d 508, 55 St. Rep. 524 (1998).

Certainly, for one party to offer money to another, but to make the exchange conditional upon surrender of something by the second party, is called a sale or a bargain.

If the right to privacy citizens have reserved to themselves can be sold by State government agents or entities, then obvious questions suggest themselves: How much can the State get for sale of the freedom of speech? How much for trial by jury? How much for freedom of the press? How much will the State garner at the citizens' rights yard sale for our right to access to justice? How high will the bid go at the auction for our right to a clean and healthful environment? How many dollars will surrendering our right to keep and bear arms bring into state coffers? Would it be simpler to just wholesale the entire Montana Constitution to the highest bidder?

One of the issues to consider in answering the question posed in Interrogatory No. 12 is, what is privacy?

Privacy is defined in a number of authoritative sources. Paraphrasing the author of the Montana right to privacy, Bob Campbell (see above), in conjunction with the *Long* decision, privacy may be defined in Montana as "freedom from government snooping." Blacks Law dictionary, Fifth Edition, defines "Privacy, right of" as follows:

> The right to be let alone; the right of a person to be free from unwarranted publicity. Term "right of privacy" is a generic term encompassing various rights recognized to be inherent in the concept of ordered liberty, and such rights prevent governmental interference in the intimate personal relationships or activities, freedoms of individual to make fundamental choices involving himself, his family, and his relationship with others.

The Random House Unabridged Dictionary defines privacy as: "pri•va•cy 1. the state of being private; retirement or seclusion. 2. the state of being free from intrusion or disturbance in one's private life or affairs: the right to privacy."

From Wikipedia, the free encyclopedia:

> Privacy is the ability of an individual or group to keep their lives and personal affairs out of public view, or to control the flow of information about themselves. Privacy is sometimes related to anonymity although it is often most highly valued by people who are publicly known. Privacy can be seen as an aspect of security—one in which trade-offs between the interests of one group and another can become particularly clear.

The right against unsanctioned invasion of privacy by the government, corporations or individuals is part of many countries' laws, and in some cases, constitutions or privacy laws. Almost all countries have laws which in some way limit privacy, for example taxation

normally requires passing on information about earnings. In some countries individual privacy may conflict with freedom of speech laws and some laws may require public disclosure of information which would be considered private in other countries and cultures.

> Privacy may be voluntarily sacrificed, normally in exchange for perceived benefits, but often with little benefit and very often with specific dangers and losses. An example of voluntary sacrifice is entering a competition; a person gives personal details (often for advertising purposes), so they have a chance of winning a prize. Another example is where information voluntarily shared is later stolen or misused such as in identity theft.

Wikipedia also says, "The right to privacy is the right to control property against search and seizure, and to control information about oneself." Continuing, "The right to privacy is the right to control information about yourself in two situations. You have the right to exclude information about yourself and you have the right to be left alone (Business Law, PBS episode aired December 15th)."

From the U.S. Department of Energy, Oak Ridge National Laboratory http://www.ornl.gov/sci/techresources/Human_Genome/publicat/genechoice/glossary.html privacy: The condition of being left alone, out of public view and in control of information that is known about you.

The protection of privacy does not stretch to include information about a person that the person himself or herself places in the public domain, such as publishing a phone number and address in a telephone directory circulated to the general public. Yet even in this example, people may elect for privacy reasons to have an unlisted phone number or to not list their residence address in the phone book, as do many single women, law enforcement personnel, celebrities, and judges.

So, there is no question that personal privacy is reserved from government interference. The various definitions tend to agree that privacy means freedom from intrusion, anonymity, and the ability to restrict and control what is known about oneself.

Social Security Numbers are assigned by the United States government as a means of identifying individuals - to keep individual identity separate and unconfused with that of

others, and to specifically be able to separate, identify, and locate every individual. This becomes especially important, both positively and negatively, in this electronic, digital age, when computers are used to accumulate, interchange, sort, store and quickly regurgitate vast amounts of data. Computers sort data by numbers.

In this computer age, a unique identifying number, such as the ubiquitous SSN, has become essential to tracking one's identity. SSNs are the common denominator by which many entities, especially including government agencies, store and retrieve information about individual people. SSNs are used by government agencies to centralize and organize access to a wealth of information, a dossier, about every individual citizen. Thus, a person's SSN becomes the key to computerized access to many confidential details about every citizen.

Are SSNs considered to be more private that other personal information, such as name, mail address or phone number? As a matter of public policy, Montana law recognizes the uniqueness of SSNs as identifiers, and as inordinately sensitive and private information.

> 61-5-127. (Effective October 1, 2007) Providing lists of licensed drivers and holders of Montana identification cards to clerks of district court -- jury selection purposes. (1) On the second Monday of May of each year, the department shall submit to the clerk of the district court of each county a list, prepared from the department's databases of licensed drivers and holders of Montana identification cards, showing the name, address, and date of birth of all licensed drivers and holders of Montana identification cards, authorized by 61-12-501, who are 18 years of age or older and whose address is in that county. The list must be compiled on a county-by-county basis and be further divided by the city of residence of the persons named on the list to enable the drawing of lists for city courts that are composed of only those residents living within a city's jurisdiction. The list must be provided for the exclusive purpose of making a list of persons to serve as trial jurors for the ensuing year.
>
> (2) The list submitted by the department under subsection (1) must be certified by the attorney general or the attorney general's designee.
>
> (3) The department may not provide the social security or driver's license numbers of persons on the list for any purpose.

And:

> 32-6-306. Personal identification number -- restrictions. (1) A financial institution may not assign a personal identification number to a customer which is identical to that customer's social security account number, driver's license number, or any other number assigned for other purposes to that customer.
>
> (2) A satellite terminal may not be operated so as to print a customer's personal identification number on the humanly readable receipt furnished at the time of a transaction.

On March 21st of 2000, Elizabeth Baker of the Montana Department of Justice (DOJ) wrote a letter to Joe Kolman of the Billings Gazette, responding to a request by Kolman for a variety of information from DOJ, including information about concealed weapon permit applicants, which included the SSNs of applicants. (Text of letter attached.) In responding, DOJ was balancing the competing interests of the right to know and the right of privacy. Acting as an official for DOJ, Baker determined that DOJ would provide "the name, city of residence, and permit expiration or revocation date of individuals who have received concealed weapon permits." However, DOJ determined that it would not provide the SSNs of applicants, notwithstanding the Montana right to know, because of the constitutional constraints of the right to privacy in Montana. No subsequent AG Op revises this standing DOJ policy.

Further, the Attorney General has barred release of SSNs by governmental entities: Availability of Payroll Record Information -- Social Security Number Excepted: Applying the balancing test set out in 42 A.G. Op. 64 (1988), the Attorney General concluded that payroll record information reported to the Department of Highways (now Department of Transportation), including the names, addresses, and wages of private employees working on a publicly funded project, is subject to public disclosure. Social security numbers of those employees are not subject to public disclosure. 43 A.G. Op. 6 (1989).
Under *St. v. Boyer*, 2002 MT 33, 308 M 276, 42 P3d 771 (2002), the Supreme Court considers three factors when determining whether there has been an unlawful government intrusion into one's privacy: (1) whether the person has an actual expectation of privacy;

(2) whether society is willing to recognize that expectation as objectively reasonable; and (3) the nature of the state's intrusion.

FWP sells lists of hunting license applicants. The statute that controls this, 2-6-109, M.C.A., does not specifically bar FWP from divulging applicants' SSNs. Under this statute, if there is any extant bar to leakage of applicants' SSNs, it is only department policy, subject to redefinition by department staff. Nor does the state policy of making records available, 2-6-110, M.C.A., specifically prohibit release of SSNs.

Certainly, Montana law defines SSNs as personal identifying information, at 2-17-551(6)(e), M.C.A., 30-14-1702(4), M.C.A., and 30-14-1704(4)(b)(i)(A), M.C.A.

So, in the Montana Constitution the people have reserved to themselves the right to privacy. This means the ability to control personal information about themselves. Because SSNs are such unique identifiers of individual persons, Montana law recognizes SSNs as a special class of data, warranting special protections under the law. If SSNs are so unique, if they constitute a special class of information about individuals, since SSNs are the common denominator to peeling open a person's identity, then requiring that a person divulge their SSN to obtain a government service or boon, or to exercise a privilege or right, must therefore be in violation of the right to privacy in the Montana Constitution. That the State is in a position to gain or lose money if this privacy intrusion is or is not effected is an argument that does not bear upon whether or not the Constitution may be violated by the State.

This discussion would not be complete without mention of identity theft. Identity theft may be a side issue in relation to the constitutional arguments raised. However, the State will argues that the constitutional issues must be mitigated by the State's desire for federal money. The State will argue that a "compelling state interest" must be met because the State has such an urgent "need" for federal money. If any such mitigation is considered, the offsetting factor of identity theft must also be considered.

Identity theft is said to be the fastest-growing crime in America. Thousands of people have had their financial lives ruined, have been made homeless, have had their

careers ruined, and have lost their families because of identity theft. Further, law enforcement response to identity theft is a hit and miss proposition. Most law enforcement agencies find little jurisdiction and little justification to pursue identity theft aggressively. Local agencies lack the tools and budget to pursue extraterritorial crime. State and federal agencies largely view identity theft as a local issue.

As a result, all law enforcement agencies from the local police department to the FBI warn people to be wary of identity theft, as if prevention is the only acceptable approach to identity theft. Further, all law enforcement agencies universally warn citizens that the best measure to prevent identity theft is to guard personal information. At the top of the list of information that we are warned to keep secret are our SSNs.

So, all law enforcement agencies warn us to not give out our SSNs, to protect against the fastest-growing crime in the U.S., yet Montana law requires us to give our SSN to an unknown, temporary employee of a local hardware store in order to obtain a license to catch one fish in Montana. That is simply irrational. To effect one's constitutionally-protected heritage to hunt or fish in Montana, one must violate all respected advice and expose oneself to a life-shattering crime.

INTERROGATORY NO. 13: For each of the Plaintiffs Marbut and Latta, please state whether they have provided their Social Security Numbers on a wildlife conservation, hunting, fishing or trapping license application on or after March 1,2000, the years of the application and the type of application.

ANSWER: Unknown. In May, 2002, I sent a letter to Nancy Kraft of the licensing division of FWP. I applied for a special permit with FWP, supplied ALS number and Elk License Number, but declined to provide an SSN. Applications for my son and myself were in the same envelope, with one check to pay for both. Both applications were rejected as being incomplete because my SSN was not provided.

INTERROGATORY NO. 14: Please state what information you have supporting your claim that Defendants have failed to provide adequate and necessary safeguards need for the preservation of Plaintiff's constitutional right to privacy.

ANSWER: The fact that the State requires State possession of a hunter's or angler's SSN at all as a condition of licensure is a violation of the right to privacy. See answer to Interrogatory No. 12. While the State asserts that it is careful with applicants' SSNs, the system of care afforded this private information is so loose as to be ludicrous. Once the State determines to collect, transfer, use and store SSNs from citizens, the doors are flung wide open to a host of security and privacy problems that the State is unable to control or even manage well.

The security and privacy problems raised by State use of citizens' SSNs may be divided into several general categories: 1) data collection, 2) data transfer, 3) data storage, 4) data use, 5) data disposal, and 6) abuse detection and enforcement. These must be addressed separately.

1) Data Collection

FWP sells hundreds of thousands of hunting and fishing licenses each year. For every person purchasing a license since 2000, FWP has required the applicant to submit an SSN. While the Automated Licensing System (ALS) purports to capture an SSN only the first time a person applies for a license, nevertheless, EVERYONE sold a license since 2000 has been commanded to provide their SSN or face refusal to grant a license.

Most of these licenses are sold by FWP License Agents (LA). License agents are sporting goods stores, hardware stores, gift shops, gas stations, convenience stores, and other retail establishments. It is common knowledge that LAs hire seasonal or temporary personnel to handle the extra traffic associated with license sales, especially in the month preceding the opening of big game season. There are no security standards for these private-sector, low-paid employees. They are not screened with criminal records background checks, they are not screened with credit history checks, and if permanent employees, they are not periodically rescreened for security purposes. Further, there is no universal system in place to prevent these personnel from abusing SSNs they gather, or to detect abuse of SSNs they gather.

It may be said that it would be impossible to require LAs to employ only people to handle this sensitive data who have the equivalent to a government security clearance. This simply points out the impossibility of adequately securing SSNs once the State has embarked on a program to require them for people to legally hunt and fish.

Some licenses are sold by FWP personnel. These personnel are also not subject to any standard and periodic security screening. For example, consider an FWP receptionist who also sells licenses at an FWP office. How would FWP know if this receptionist has run up $50,000 in gambling debts, is not paying usual bills, and has become an easy mark for identity theft criminals? If this receptionist should weaken and begin providing sensitive personal information, including SSNs, to criminals, what detection strategy and procedures are in place to nip such activity in the bud?

2) Data Transfer

Most hunting and fishing licenses are sold by License Agents, franchised by the State. Once the SSNs of applicants are collected, they are both transmitted to FWP and stored locally. The LA retains a copy of a paper license application. The LA sends another copy of the license application to FWP. There are security problems with this process. There are no recognized security levels or procedures applied to LAs for their storage of license application copies. There are no recognized security levels or procedures applied to the transfer of license application copies from the LA to FWP. They are simply mailed. In the State's reply to Interrogatory N. 12 by Plaintiffs, at the bottom of Page 8 of the State's Answer, the state says, "The mail containing the application is opened and checked, it is them batched and the information data entered into the ALS system." Who opens the mail? Is the mail opener a minimum-wage clerk, or a veteran FWP staffer with a security clearance? When the applications are "batched", does this mean that a pile of applications are left sitting on somebody's desk until FWP personnel get around to entering the data into computers?

For those applications that are entered into a computer terminal at the point of sale, is the data transferred to FWP according to accepted encryption standards, such as Triple

Defense Encryption Standard (3DES) with a minimum 128-bit encryption key? Is the data transferred over standard phone lines, or secure and dedicated lines?

Of course, having a universally secure method of transmitting this data from individuals to the State would be troublesome, probably even cumbersome. This only points out again the folly of requiring citizens to supply such sensitive data as an SSN in order to be given permission by the State to hunt and fish legally in Montana.

3) Data Storage

Storing citizens' SSNs suggests a whole new set of problems. It is with data storage that the greatest threat to security exists. Most data theft and data loss events have to do with breaches or failures of data storage.

The State asserts in its Answer to Plaintiffs' Interrogatory No. 12, at the top of Page 9, that paper copies of license application "are sent to records storage with a 3 year retention." There is no description of what "records storage" amounts to. Are boxes stacked in a basement hallway of the FWP building? Are records stored in a shed behind the FWP building? How many people have access to "records storage"? Are security clearances required for people with access to this records storage area? Can the records storage be physically secured? If so, is it always kept secured, or is it usually left unlocked for access convenience? Is the records storage area restricted to access by FWP personnel only? If not, how many other people have access to this storage?

One gleans from the State's answers to Plaintiffs' Interrogatories that much of the sensitive personal data, including SSNs, stored by the State is stored in electronic form. Of course, there is a host of potential problems associated with the security of data stored electronically. Electronically-stored data is subject to some additional principles of security. Although additional security strategies may be applied to the security of electronic data, breaches of security can be much more disastrous, because vast amounts of data can be pilfered, even remotely, in a very brief period of time.

One large problem is controlling who has access to secured data, or who has access to computer terminals that can access secured data. In the State's Answer to Plaintiffs'

Interrogatory No. 15, the State asserts that business hours access to the building where citizens' SSNs are stored or may be available has this control feature: "... DPPHS CSED entrances are staffed by receptionists who admit access only to authorized persons." This places simple receptionists in the role of security personnel. Are these receptionists trained and licensed as security personnel?

"HELENA - A computer was stolen from a state health department office here earlier this week, and state computer experts were unable to say Friday if the computer held any sensitive information because they had not been informed of the theft." (Associated Press, 07/07/2006.)

Further, on Pages 9 and 10, the State admits that citizens' SSNs are available from satellite offices in Great Falls, Butte, Missoula, Billings and Helena. No mention is made of what physical security is present at these widely-dispersed locations.

In the State's Answer to Plaintiffs' interrogatory No 12, in the bottom half of Page 8, the State admits that paper applications for various licenses are stored at FWP regional offices. Absolutely no mention is made about how long these forms are kept, how they are secured, who has access to them, and more. This is yet another major hole in the State's privacy net, and again highlights why SSNs should not be collected in the first place.

On Page 12, in Answer to Interrogatory No. 18, the State admits that there is physical access to data storage by "computer operators and operations support staff, computer systems engineers and systems administrators, database administrators and telecommunications specialists." Further, the State admits, "In addition, there are numerous other state employees and contractors with various types of physical access including facilities managers, facilities maintenance staff, security guards, computer maintenance vendors, etc."

In February of 2005, the Legislative Auditor released a report on his audit of the Department of Fish, Wildlife and Parks' (FWP) Automated Licensing System (ALS), the computer operated electronic system by which license applications are entered into the system, data is transmitted, and data is stored on State computers (Audit 05DP-03).

In describing the ALS, the report stated:

The system issues licenses and permits using point-of-sale (POS) terminals at license provider locations that communicate with servers housed and maintained by the State of Montana's Information, Technology Services Division (ITSD). ALS users include FWP employees and contractors (and their employees - G.M.) who develop and administer ALS, internal FWP providers who issue licenses at FWP headquarters and regional offices, external license retailers (and their employees - G.M.) who issue licenses from their business locations, and public users who access ALS from the web.

One of the issues examined by the audit was the extent to which excess ALS access privileges were granted and maintained. The audit concluded that far too many people have administrative access to the system, that the areas of system access are far more broad than needed for specific authorized individuals to perform job functions, that lists of those with access codes are not monitored, that persons no longer needing access do not have access privileges revoked, and more. It is worth quoting the findings of this audit in some detail.

We reviewed access privileges for the administrative application granted to select department administrators, licensing personnel, operations personnel, development personnel, and contractors. For the six users examined, access was identified that was unnecessary to fulfill the users' job functions. We confirmed the unnecessary access with the ALS personnel, who acknowledged the problem and stated that access needed to be "cleaned up". Personnel indicated that the user portion of the production database was probably copied over from the development database when they went live in 2002.

Industry standards state that management should implement procedures that provide access security control based on the individual's demonstrated need to add, change, or delete data, and should have a control process in place to review and confirm access rights periodically via periodic comparisons with recorded accountability.

Unnecessary access to system screens and data enable a user to perform functions not related to job duties. Users can access and change data either accidentally or

intentionally. The procedures to grant user access to the administrative application are not documented. No periodic review of user access privileges for appropriateness is performed, which would facilitate the identification and removal of inappropriate user access. During our fieldwork, ALS personnel could not trace 3 contractor User ID's back to an actual contractor.

Additionally, when a new user is created in the administrative application, the user is given, by default, excessive privileges for the underlying tables in the ALS production database. Users who directly access the database outside of the administrative application have the ability to insert, update, and delete (and copy - G.M.) any ALS data in the database. FWP personnel stated this was a design decision made for the sake of simplicity, and no second thought was ever given to changing it until now.

This is a considerable list of people with electronic or physical access, some very non-specific, such as "contractors" (including their personnel), "vendors" (including their personnel), maintenance staff (janitors, one presumes), and "etc." (and their personnel?) It would seem that access to the areas where sensitive data are stored is available to a wide range of State employees, and a whole bunch of other people who only need the magic words of "contractor", "vendor", "staff", or "etc." in order to obtain access. This is not what any reasonable person would call "security".

The State admits in its Answer to Plaintiffs' Interrogatory No 14, on Page 9, that many people who have access to SSNs collected from hunters and anglers do not have background checks, and the State makes no mention of periodic background checks for those who undergo initial background checks.

In June of 2006, the Legislative Auditor released its report of its audit 06DP-05, "Data Center Review". (http://leg.mt.gov/content/audit/download/06DP-05.pdf) This audit examined various security measures and procedures applied by the Department of Administration (DoA) to its central "Data Center," the location where vast amounts of sensitive state information, including citizens SSNs, are stored.

The report pointed to lack of threat analysis:

DofA has not identified and documented threats to the data center, determined threats that are not addressed by a control, or determined the need for controls to address an existing threat or vulnerability. Physical security threats were disclosed by an independent security assessment report in 2002, but the office responsible for physical security, the Office of Cyber Protection (OCP), was unaware that the report existed. Efforts to implement controls have been limited to damage control and remediation as problems arise rather than a formal proactive approach to determine the adequacy of the control based on risk and cost analysis. Risks, including likelihood of occurrence and potential impact associated with threats, have not been determined or evaluated.

The report noted absence of background checks for personnel with access to the Data Center:

DofA does not have controls in place to ensure all DofA employees in positions requiring background checks have those checks completed. According to Section 44-5-405(1), MCA, "Personnel, applicants and current employees that work with or in a computer center that processes criminal justice information are subject to a background check." The data center transfers information used by the Criminal Justice Information Network (CJIN) system. We reviewed individuals with data center access and identified 91 individuals without background checks. These individuals consisted of 52 DofA staff and 39 staff from other agencies. There is no process to ensure all employees with the defined job positions have background checks completed or procedures for regularly reviewing employees in the defined job positions to ensure the background checks are completed.

The Report also noted a lack authorization documentation for persons accessing the Data Center:

The department has an internal policy to authorize data center key card access. Each person with data center access should have an authorization form on file with justification of which doors need to be accessed, why the access is necessary, and approval signatures from the individual's supervisor as well as the CIO. We reviewed access for all

active key cards, to confirm the internal policy was being followed. Authorization forms for individuals with access to the outermost door of the data center were on file for 21 of the 144 active key cards, while the innermost door had 7 of 121 authorization forms on file. OCP personnel explained that due to moving of personnel and office space, the documentation has been lost, and lack of consistent understanding of what forms are necessary to request access also contributed. Some people request access via email or submitting a request to the DofA help desk. Neither of these options complies with the internal policy requirement of an approval signature from the CIO.

DoA allows visitors to access the Data Center, but has essentially no effective controls implemented to monitor or constrain visitor access.

The use of visitor key cards is required in policy, but enforcement has not been required. Visitor logs are located outside the perimeter data center doors, but no controls are in place to ensure the logs are filled out or accurate. The logs reside in a publicly-accessible area, and are not reviewed. Without the use of key cards and review of the visitor logs, visitor entry to the data center can occur for any reason and will not be known by OCP, who is responsible for physical access to the data center. DofA does not have controls in place to detect patterns of inappropriate visitor access.

Finally, the report points out that operating personnel at the Data Center are focused almost exclusively on providing convenience and service to other State agencies, at the expense of securing sensitive data.

DofA staff noted on several occasions reasons for controls not being in place included a preference to provide convenient services to the agencies as opposed to putting security as a priority. We were informed of instances where security measures were not given a high enough priority or enough time to do what was necessary and on occasions access is granted based on convenience for contractors and agency personnel. Security to the data center, which houses some of the most sensitive and critical data in state government, should be controlled by a principle of least access approach, rather than allowing convenient accessibility.

Certainly, it would be difficult for the State to maintain rigid and reasonable physical security over all of the areas in the State where citizens' SSNs are stored or available. This further underscores the folly of collecting SSNs in the first place.

Let us turn to discussion electronic security.

HELENA - The state computer system building, and the taxpayer information and other sensitive data it holds, are vulnerable to security breaches, legislative auditors told lawmakers Tuesday.

The audit came one day after the state computer system's second failure in less than a month. (Associated Press, 06/20/2006)

See Data Center Audit 06DP-05 (http://leg.mt.gov/content/audit/download/06DP-05.pdf)

HELENA - A key legislative committee told the Martz administration Wednesday it should pull the plug on remnants of a problem-plagued and undependable computer system that has cost the state $37 million and still doesn't work properly. (Associated Press, 12/19/2002) 44-5-403. M.C.A. establishes a standard for security for computer programming for criminal justice information.

44-5-403. Computer programming. Procedures for each automated criminal justice information system shall assure that the information is secured by the following programming techniques and security procedures:

(1) the assignment of a terminal identification code to each terminal authorized to access the criminal justice information system;

(2) the assignment of a unique identification number to each authorized terminal operator, which number must be used to gain access to the files;

(3) the maintenance of a record of each inquiry to identify the inquiring agency, the program used to make the inquiry, the date of the inquiry, and the name of the file being queried;

(4) computer programming controls to ensure that each terminal user can obtain only that information which the user is authorized to use;

(5) creation and use of a safe place for storage of duplicate computer files;

(6) built-in program controls to ensure that each terminal is limited to the appropriate or authorized information that can be input, modified, or canceled from it;

(7) destruction or safeguarding of system documentation and data input forms; and

(8) creation of reports to provide for an audit trail and periodic review of file accessed, modifications, and deletions. All criminal justice intelligence information shall be identified as such.

This level of caution appears not to be observed concerning citizens' SSNs stored by the State. At least, this standard is not mentioned in the State's Answer to Plaintiffs' Interrogatories. Criminal justice information may be seen to contain two different types of sensitive information: 1) private information relating to persons subject to the criminal justice system, and 2) State secrets which the State wishes to keep under careful control. Is it that the State cares less about the privacy of non-criminal citizens than it does about the privacy of persons subject to the criminal justice system, or is it that the State cares more about keeping its own secrets than it cares about the citizens? Certainly, this dichotomy of treatment suggests that the State cares less, or is careless, about the security it applies to the private information it coerces from citizens, SSNs.

GREAT FALLS - Montana's foster care system fails to meet national standards in two key areas, but state officials say it is a computer data and reporting problem, not an issue of care. (Associated Press, 12/25/2004)

In its Answer to Plaintiffs' Interrogatory No 6., the State admits that it released hunter and angler license information to a dozen entities in 2005, but seems to infer that its collective memory fails to recall any previous releases.

According to the Congressional Sportsmen's Foundation, in partnership with the National Shooting Sports Foundation, (http://www.sportsmenslink.org/Sportman/state.html#) it is estimated that Montana sells about 229,000 hunting licenses each year, and about 349,000 fishing licenses. This totals 578,000 licenses. If FWP released this data to 12 different entities in 2005, then it

released 6,936,000 records in 2005 alone. Excusing FWP's poor memory about previous years, and supposing it released the same volume of data in 2000, 20001, 20003, 2004, 2005 and 2006, then FWP has released the personal information of 41,616,000 hunters and anglers to entities outside FWP. And, these releases are only the ones FWP admits, remembers or can be directly inferred. Although FWP brags that it does not release hunters and anglers SSNs, with this incredible volume of data outflowing from FWP it becomes difficult to take seriously the claim that no citizens' SSNs are ever released. Mistakes happen. This is yet another reason why it becomes an affront to privacy for the State to require and collect SSNs in the first place.

One significant error is noted in the State's Answer to Plaintiffs' interrogatory No 12, at the top of Page 6. The State asserts, "The Federal Government (42 USC 666 (a) (13)) authorizes states to require SSNs on applications ..." This is incorrect - actually a lie. First, Congress cannot authorize, has no authority to authorize, a state to do anything which is in conflict with the state's own constitution. Secondly, 42 USC 666 (a) (13) only has the effect that a state may become ineligible to receive certain federal dollars if it fails to collect citizens' SSNs, substantially different than *authorizing* anything.

Further, the State asserts in its Answer to Plaintiffs' Interrogatory No. 12 that SSNs sent to FWP electronically by License Agents are encrypted, but it fails to specify if any recognizable standard for encryption is used. There are many process available that can be called encryption. Many of them are not valid encryption and do not provide a significant level of security. The industry standard used by banks and financial centers is encryption with a 128-bit encryption key and algorithm. Another standard is the Triple Defense Encryption Standard (3DES). The State fails to assert that any viable encryption standard is used, only that data is encrypted. One might assume that if any really viable encryption standard were being applied, the State would claim and assert that standard.

Also, the State admits that citizens' personal data is decrypted by the Department of Administration for a fuzzy activity called "update." This adds a whole new group of people (DoA) to the long list of those who have access to this unsecured data, making it further

difficult for the State to adequately secure citizens' SSNs, yet another reason why collecting SSNs violates privacy.

Although the State claims that FWP does not release hunters' and anglers' SSNs to anyone besides DPHHS, for any reason, it is possible that the State is not being totally forthcoming. For example, if a person is charged with a game law violation, is the SSN of the accused released to the county wherein prosecution is requested? Also, it is noted that Montana belongs to the Interstate Wildlife (game law) Violators Compact (IWVC). This Compact, at 87-1-801, M.C.A., Article III(4) requires FWP to release "violator the information in form and content as prescribed in the compact manual." In its declaration that the State releases no SSNs except to DPHHS, it is silent about what information is required by the "compact manual." Further, it is noted that the IWVC may be amended in a way that does not require the assent of the participating state, only non-objection for 120 days to proposed amendment. Has it been amended so that the form in the M.C.A. is not current? Is FWP releasing SSNs in excess of their declaration that they only release to DPHHS? If this slippage exists, is it not yet another reason why privacy is violated if the State collects SSNs at all.

In the State's Answer to Plaintiffs' interrogatory No 12, at the top of Page 7. The State asserts, "After 5 years of non-use SSNs are automatically deleted from the System ..." In the world of computer science, the word "delete" is a word of art -- it has a very specific meaning. It is not synonymous with "wipe," "shred" or "destroy." With most computer operating systems, when the system "deletes" a file, it only changes the first character of the file name used, and *may* instruct the File Allocation Table (an index of files) that the space used by the file is available for re-use. For example, the file name of this document is "Discovery answers 0806.doc". If I were to instruct the computer to "delete" the file, the file name would be changed to something like "0iscovery answers 0806.doc". Any high school computer geek could enter the file structure and try replacing the zero in the file name with various letters. Within 26 tries (many fewer with a bit of intelligence - how many letters can the word "Discovery" start with) the geek would have the *entire* file.

Depending on the operating system, this file might be preserved forever, or it might only be preserved until the computer data storage strategy used decides it needs the available space for something else. If the State computers and operators actually do what the State claims -- "delete" files -- then the files are probably still there and the state may be in noncompliance with state laws. In any case, it generates little confidence that citizens' SSNs are really secure with the state, another reason why it violates privacy for the State to harvest and store citizens' SSNs.

In the State's Answer to Plaintiffs' interrogatory No 12, at the bottom of Page 7, the State admits that FWP also maintains "the old sportsmen's license database which lists SSNs..." The State offers no explanation about how this separate "old" database of SSNs is secured, who has access to it, where it is stored, and more, yet another reason why collecting SSNs from citizens violates privacy.

HELENA (AP) - The Montana state computer system ground to a halt Tuesday when it came under attack from a virus, one week after escaping unscathed when a similar virus-like worm hit computers around the world.

Many state services, such as license renewals at the Motor Vehicle Division, were unavailable Tuesday and many state workers were unable to get into some of the state's main computing systems. (Associated Press, 08/19/2003)

This discussion of electronic security would not be complete without mention of "hacking." Hacking is the process of breaking into a data storage system from a remote location. There are entire societies of computer hackers in the U.S., and in almost every other country in the World. Because the electronic networks are global, a data storage system like that of the State must be prepared to defend against very sophisticated hackers around the World. Most hacking is done to steal data. Data is valuable. The most notorious hacking successes have been highly sophisticated criminal gangs from China who hack computers specifically for identity theft purposes. When they are able to get into a system and get a person's name, address, *and especially SSN*, they apply for credit in the

person's name, run up huge debts in the person's name, and then vanish. Many people have been ruined because of this type of hacking and identity theft.

The State data storage which stores SSNs taken from citizens who apply to hunt or fish is obviously connected electronically, by wire or optic, with other computer systems and thereby with the rest of the World. It is vulnerable to hacking, as well as to viruses like the one described in the AP story above. In its Answers to Plaintiffs' Interrogatories, the State makes no claim to have adequate firewalls and other security procedures in place to inhibit hacking. The word "inhibit" is used deliberately because there is no absolute proof against hacking unless the target computer is totally disconnected from other computers and also disconnected from any electronic or optic incoming and outgoing data transfer mechanisms. The simple fact that SSNs are collected and stored by the State makes an inviting target for professional hacking, and risks the privacy of citizens from whom SSNs are collected.

BOZEMAN - The database maintained by the Department of Fish, Wildlife and Parks recently was broken into by a computer hacker but no data was stolen, an agency spokesman said Tuesday.

The database is loaded with personal information from hunters.

Spokesman Ron Aasheim told the Bozeman Daily Chronicle on Tuesday that the database was hacked last month, and that the hacker made it onto the server containing the state's hunter-harvest survey, personal information including Social Security numbers of hunters and information about where they hunted and what wildlife they killed. (Associated Press, 06/29/2005)

It may be impossible for FWP to know whether or not any data was taken. If someone uses a master key to gain access to your home while you are gone on vacation, turns on your computer and makes copies of data stored there, leaves the data intact, turns off your computer and relocks the door on the way out, how would you ever know that or if your data had been copied? It is likely that FWP is in exactly this position, and

that FWP assurances that "no data was stolen" comment is just bluster, or that the statement actually means that "no data was erased while it was being stolen."

BILLINGS - A computer crimes increase, so does effort to stop them. On busy days, Rich Hurlocker's beeper goes off eight times.

It's his computer calling for help. Someone is trying to break into the network of his employer, Rocky Mountain College.

Hurlocker, RMC's system administrator, drops what he's doing and runs to a computer to check the activity. Usually it's just a novice hacker probing the university's computer network for a weak spot. "It' s like people going around and trying the doorknobs on your house," he said.

There has not been an actual network break-in at RMC for two years, but the doorknob turning is becoming more determined and Hurlocker has to work harder to keep the school safe from hackers.

"It's a constant battle," he said. "It's getting worse."

Silent but fierce skirmishes between hackers and computer network administrators take place every day in Billings. They're becoming more frequent. Federal prosecutors and computer experts talked about the problem last week during a seminar on computer privacy and policy at RMC.

"How many of you have been victims of an intrusion?" Assistant U.S. Attorney Jim Seykora asked the audience of about 60 computer professionals.

Nearly every hand was raised.

The stigma of being violated and the publicity of losing secure information keeps many from reporting computer crimes, Seykora said. This lack of punishment leads hackers to believe it's OK to break into private systems. It becomes merely a game for bored computer users, many of whom are teen-agers. (Missoulian, 05/27/2001)

HELENA - A hacker may have gained access this week to some files on a computer server in the Office of the Commissioner of Higher Education, forcing officials to shut down

and reformat the server, Commissioner Sheila Stearns said. (Associated Press, 04/30/2006.)

4) Data Use

The State's claims of perfectly benign and careful use of SSNs is reminiscent of Lucy's promises while holding the football for Charlie Brown. Possession is 9/10ths of the law, it is said. Once government agencies possess this information, use and care of the information is at their discretion and out of the hands and control of the citizen to whom the information relates. It is not so much a question of how the State uses SSNs now, as how they could be used at some future date. We know that government at various levels desires to centralize all records about people, to make information about any person available with a few convenient taps on a computer terminal. The information that is becoming more centralized in government computers includes a person's name, mail address, present and past residence addresses, phone number, cell phone number, SSN, date of birth, names of parents, spouse and children, vehicle type, make, color and license number, property ownership, associations, ANY brushes with government agencies (including arrests, receipt of public benefits, licenses, permits, etc.), financial dealings, medical interactions, insurance, credit history, and more.

Since a person's SSN is usually the key to accessing any and all of the information listed above, and since the desire of government agencies and personnel is to centralize all such information, the mere possession by the State of a person's SSN violates the very essence of privacy. Perhaps being able to quickly assemble a vast amount of information about a person will not directly injure a person's privacy this week or this year, but having a system in place *capable* of doing that violates the very concept of privacy.

The government information systems are specifically designed to create a net from which no one can hide. But why would anyone want to hide if they haven't done anything wrong, it might be asked. In that case, why doesn't everyone have WebCams in their bedrooms? Why do we put our mail messages in envelopes, instead of on postcards for anyone to read? When the German Nazis disarmed the Jews before WWII, they said that

Jews had no legitimate need for a gun. If you want a gun, join the Army, they said. Of course, after they were disarmed, it was ever so easy to round the Jews up and ship them off by the trainload to concentration camps.

So why be concerned about government electronic dossiers making it impossible for anyone to hide, if they have done nothing wrong? Two reasons. The first is privacy -- having control over information about oneself. Like a secret, once information is in the hands of someone else, it is no longer one's own (Yeah, right. We're from the government and we're here to help you.)

The second has to do with the notion, "If you've done nothing wrong." We are all expected to comply with a body of laws and regulations that, if printed on paper, could not be hauled in five, over-the-road semi trucks. Ignorance of the law is no excuse, we are told. Yet no living person in the U.S. is capable of knowing all of the laws and regulations we are required to know and obey. Thus, it is unavoidable that every one of us will occasionally, and innocently, violate a law or regulation -- do something wrong.

This is where privacy becomes a buffer between the citizen and a collective government apparatus that grows more intrusive and present on a daily basis. And, this is why collecting citizens' SSNs violates privacy.

State currently lacks capability to check

By JOE KOLMAN, Billings Gazette, Records check would help law enforcement:

BILLINGS - State officials say they hope to have the capability soon to perform record checks such as the one done by the Billings Gazette to find felons who may possess firearms illegally.

"We thought your idea was pretty darn good," said Mike Cronin, spokesman for the Department of Corrections.

Officials say computer systems are just now reaching the point where they can be coordinated between state agencies.

"I know there are things we definitely want to work toward," said Shelley McKenna, a program specialist in the Department of Justice who works with the Sexual and Violent Offender Registry.

The newspaper obtained an electronic copy of that registry and compared it to hunting licenses sold last year to determine how many felons were likely in possession of weapons. (Missoulian, 05/15/2005)

5) Data Disposal

"To err is human; to forgive Divine" a thought attributed to Alexander Pope from "An Essay on Criticism." People make mistakes. Once private personal data is out of the hands of the person to whom it applies and in the hands of someone else, it is in the hands of people who will make mistakes.

Sensitive data sold with surplus state computers

HELENA — State agencies have failed to remove private information about Montanans before retiring outdated computers, risking public disclosure of such things as Social Security and credit card numbers, medical records and income taxes, a new report discloses.

The legislative audit, obtained Tuesday, blamed unclear state policy for the computer hard drives not being properly "scrubbed" before the machines were donated to school districts, given to other state agencies or sold to the public.

'The state lacks a single clear policy instructing departments on information removal, assigning responsibility for defining sensitive data, and assigning responsibility for performing data removal and certifying the task has been accomplished," the auditors said. Bob Anez of The Associated Press - 05/25/2005
http://www.montanastandard.com/articles/2005/05/25/newsstate/hjjejehejcgjjg.txt
Audit 04SP-31 available at: http://leg.mt.gov/content/audit/download/04SP-31.pdf

In that audit, the Legislative Auditor found that:

Privacy is an individual's inherent right. The Montana Constitution confirms this expectation and affirms Montana citizens' right of privacy and the state's duty to protect

this privacy. Implementing this right through statute and policy, the state is required to protect individual privacy and the privacy of the information contained within computer systems by restricting information disclosure.

The Legislative Auditor tested 18 computer hard drives from retired State computers and found that 12 of those still contained State data. The audit report says, "Eight of the 18 hard drives held information restricted from public disclosure by Montana's constitution, legal statutes, administrative rules or Federal requirements." This data included "386 social security numbers, 182 private-party financial records, 84 private-party business records, credit card numbers, health and medical information, restricted federal information, job applicant information, state employee personnel information," and "department confidential procedures (security related)."

It is the nature of a bureaucracy to accumulate vast amounts of data, to seldom dispose of any information. The State asserts that FWP "deletes" SSNs after they have been unused for five years (discussed above). The State claims that FWP shreds some paper documents containing hunters' and anglers' SSNs. Yet, there appear to be lots of different forms, in different places, that either do not get destroyed, or are not destroyed according to any particular standard of distraction. Imagine looking in the dumpster behind a regional FWP office and finding ten cartons of license applicants' application forms "disposed of" by simply throwing them in the dumpster. The State points to no effective policy that would preclude such an incident.

The same may be said for the disposal policies of the many FWP License Agents across the state, and the copies of paper license applications they keep.

The State is also silent about disposal of the paper copies of FWP database queries done by DPHHS personnel from all over the state who have access to the FWP database and hunters' and anglers' SSN. Are these printouts simply thrown into the nearest wastepaper basket when they are no longer needed.

The State's Answers to Plaintiffs' Interrogatories suggest (as does common sense) that the State has a backup strategy for backing up data on State computers. Yet no policy

is provided about what becomes of backup storage media (tapes, optical disks, etc.) when it is obsolete. And, if some sort of policy is in place, who insures that the policy is properly executed? These are all good reasons why the State should not be collecting SSNs, for citizen privacy reasons.

6) Abuse Detection and Enforcement

Suppose a state employee, an employee of an FWP license vendor, an employee of a firm contracted by the State for technical computer services, or even a computer-savvy janitor, should fall on hard times, any one of the scores of people with access to SSNs collected and stored by FWP. Suppose this person hears of an identity theft ring that will pay $.10 each for current records of citizens name, address, and SSN. This person could stand to make a quick $58,000 by somehow intercepting, copying and selling the information from the licenses FWP issues each year. FWP makes this convenient by storing all this data in one place, in an easily copyable electronic format. If this person quietly and cannily makes a copy of the 578,000 license applicant records onto one optical disk, how is this data theft to be detected?

If it is detected, who will have enforcement authority. Suppose this happens remotely from a Billings DPHHS office. Will the Billings Police Department investigate, or the Yellowstone County Sheriffs Department. Or will that be up to the Helena Police Department or the Lewis and Clark County Sheriffs Department because the data actually resided in Helena? Do any of these people have experience, training, or certification in detecting and investigating cybercrime? Will Department of Justice investigators become involved? If so, what is their expertise in cybercrime? Can and should federal investigators be called in if this happens wholly within Montana?

If the thief has already passed the information along to an identity theft gang in China, how will any investigation or prosecution help the Montana citizens subsequently targeted for identity theft? The only thing the state could do at that point would be to warn hunters and anglers that their privacy and security had been compromised, as was done recently when data broker Choice Point sold tens of thousands of personal files to an

identity theft ring, or when a Veterans Administration computer was recently stolen, along with the personal information and SSNs of 26 millions military veterans. (http://www.worldnetdaily.com/news/article.asp?ARTICLE_ID=50328.)

Detection and obstruction of amateur hackers is doable. Detection and obstruction of professional hackers is problematic and uncertain. Law enforcement against hackers is almost nonexistent. Detection and obstruction of common thieves is uncertain also, witness the theft of the DPHHS computer, which theft remained undetected for days. The news media have not yet reported any conclusive enforcement action against this thief.

A 2005 audit of the Information Technology division of the Montana Department of Administration by the Legislative Auditor found that state laws and policies for data protection were not being implemented or enforced (Audit 05DP-06). The audit report says that DoA practices fail to comply with the Montana Information Technology Act (MITA), "Of the sixteen sections of MITA that fell under the scope of this audit, nine are not being implemented and enforced to the intent outlined in state law." The report says, "The department has not actively addressed issues of enforcement for agency non-compliance with policies, decisions, or even the statutes established within MITA." The report also states, "Documentation of rules, policy and procedures is minimal and inconsistent."

State operation, maintenance and security of computer data handled by the State is a mess. It is a sieve of a system full of major holes in compliance with state law, standard practices and security procedures. FWP already admits that its computers storing private personal information and SSNs have been broken into (Associated Press, 06/29/2005), yet corrections sufficient to guarantee data security have not been implemented.

Because the State cannot adequately detect and enforce against data theft, at least not sufficient to offer any security guarantees, the State should not be collecting and storing the SSNs of hunters and anglers at all. This is another reason why such collection and storage violates the right to privacy that the citizens of Montana have reserved to themselves.

INTERROGATORY NO. 15: Please state what safeguards Plaintiffs consider adequate and necessary to preserve their right to privacy in the implementation of the Social Security Number requirement of MCA § 87-2-106 and §87-2-202.

ANSWER: None. Discontinue requiring SSNs for hunting, fishing and trapping licenses. Discontinue collecting SSNs in any way, for any reason. Destroy all paper records existing anywhere that contain applicants' SSNs. Purge all SSNs from State computer systems with a DoD-quality scrubbing program. Physically destroy all backup records, electronic, paper or otherwise, with DoD-quality records destruction techniques. Require License Agents to destroy (not dispose of) all paper records on hand and in storage. Redesign ALS software so SSNs are not involved in license application. Redesign license application forms so SSNs are not requested.

To continue collecting and storing SSNs and doing that with adequate security - to do it right - would be far too expensive and cumbersome for the State, would be too difficult for the myriad of employees the State has working and others not employees of the State, who now have ongoing or occasional access to citizens' SSNs.

DPHHS has testified to the Legislature that they do not utilize their option to query the FWP database looking for "deadbeat dads" denominated by SSN. They have testified in legislative committee hearings that they only need SSNs collected and stored by FWP to remain in compliance with federal mandates for eligibility for federal money. So, collecting SSNs from hunting, fishing and trapping license applicants is not helping any children in Montana, it is only helping DPHHS maintain eligibility for federal money, nearly all of which is used for staffing at DPHHS. Said more directly, the people at DPHHS who have so adamantly supported the collection of SSNs at the expense of privacy for Montana citizens have a clear conflict of interest. Their jobs are funded by the federal dollars at issue. For their employment incomes, it seems desirable to them to sacrifice the Right to Privacy that the people of Montana have reserved to themselves in the Montana Constitution.

Because of the very questionable to poor integrity of the various parts of the State computer system (see above), because the State cannot afford to hire personnel of a level

of competence necessary to absolutely secure sensitive data like citizens' SSNs, because of the extreme difficulty of detecting and enforcing against data theft (see above), and because so much of the security of SSNs is outside the control of the State (see above), there is no set of policies and practices the State could adopt that would satisfy this Plaintiff that the constitutional right to privacy is being adequately protected as long as the State continues to collect and store SSNs for citizen license applicants.

REQUESTS FOR PRODUCTION

REQUEST FOR PRODUCTION NO. 1: Any and all documents that you or anyone acting on your behalf contends or believes support or relates to any allegations set forth in your Complaint.

RESPONSE: To the extent that such documentation exists, it is attached hereto and bates numbered 1 through 649. In addition, Plaintiffs continue to diligently search for such documentation in their own records and are seeking such documents from Defendant and other witnesses. To the extent such documents are discovered in future, this response will be supplemented.

REQUEST FOR PRODUCTION NO. 2: Any and all letters, email, email records, electronic documents, correspondence, writings, or there documents relating, in any way, to any allegation set forth with particularity in the pleadings in this case (if any documents are withheld based on a claim of privilege, please produce a privilege log identifying said documents by date, author, recipient, and anyone who received copies of such document).

RESPONSE: To the extent that such documentation exists, it is attached hereto and bates numbered 1 through 649. In addition, Plaintiffs continue to diligently search for such documentation in their own records and are seeking such documents from Defendant and other witnesses. To the extent such documents are discovered in future, this response will be supplemented.

REQUEST FOR PRODUCTION NO. 3: Any and all electronic messages or documents, email, email records, deleted email, draft email, saved email, email located in

the "Trash" or "Recycle Bin," email fragments, email correspondence, email attachments, and all other electronic documents and files related to this matter.

RESPONSE: To the extent that such documentation exists, it is attached hereto and bates numbered 1 through 649. In addition, Plaintiffs continue to diligently search for such documentation in their own records and are seeking such documents from Defendant and other witnesses. To the extent such documents are discovered in future, this response will be supplemented.

REQUEST FOR PRODUCTION NO. 4: Please provide documentation for each and every instance you list in your responses to preceding Interrogatories.

RESPONSE: To the extent that such documentation exists, it is attached hereto and bates numbered 1 through 649. In addition, Plaintiffs continue to diligently search for such documentation in their own records and are seeking such documents from Defendant and other witnesses. To the extent such documents are discovered in future, this response will be supplemented.

REQUEST FOR PRODUCTION NO. 5: Please provide a copy of each and every civil and criminal investigatory reports (sic) and notes (sic), court pleadings (sic) and documents, (sic) statements (sic) to the press, and any other written or orally recorded information concerning the allegations in paragraph 15 of the Complaint.

RESPONSE: To the extent that such documentation exists, it is attached hereto and bates numbered 1 through 649. In addition, Plaintiffs continue to diligently search for such documentation in their own records and are seeking such documents from Defendant and other witnesses. To the extent such documents are discovered in future, this response will be supplemented.

REQUEST FOR PRODUCTION NO. 6: Please provide a copy or description of security measures Plaintiff's (sic) believe are necessary and adequate to prevent unauthorized disclosure of their Social Security Numbers.

RESPONSE: To the extent that such documentation exists, it is attached hereto and bates numbered 1 through 649. In addition, Plaintiffs continue to diligently search for

such documentation in their own records and are seeking such documents from Defendant and other witnesses. To the extent such documents are discovered in future, this response will be supplemented.

REQUESTS FOR ADMISSIONS

REQUEST FOR ADMISSION NO. 1: Admit that the state statutory requirement to provide a Social Security Number when applying for a wildlife conservation license or a hunting, fishing or trapping license became effective for license years beginning March 1, 2000.

RESPONSE: Denied. FWP was demanding SSNs for special permit applications in violation of a clear reading of the law. Montana law only allowed FWP to demand SSNs for Conservation Licenses. Beyond that, FWP was operating in excess of the law, abridging the constitutionally reserved right to privacy by simple agency fiat, without authority. When I applied for a special permit in 2002, I was excluded from the drawing process because I declined to provide an SSN for what was an agency fiat. It is admitted that FWP, because of my protest, eventually removed the SSN requirement from special permit application forms, but not until I had been injured by FWP exclusion from the process and opportunity. Upon invitation to do so, FWP failed to articulate anything it could or would do to make me whole from that injury.

REQUEST FOR ADMISSION NO. 2: Admit that the alleged identity theft of Carol Latta occurred several years before the effective date of the state requirement to provide a Social Security Number on a wildlife conservation or hunting, fishing or trapping license application.

RESPONSE: Unknown.

REQUEST FOR ADMISSION NO. 3: Admit that the requirement to provide a Social Security Number on wildlife conservation and hunting, fishing, and trapping license applications is a requirement of federal law as a condition to the state's receipt of federal public assistance and child support enforcement funds.

RESPONSE: Denied in part. It is a Montana statute that prevents FWP personnel and agents from selling me a conservation law if I decline to provide my SSN. The Montana Legislature had a choice about whether or not it imposed this privacy erosion upon hunters and anglers in Montana. It chose to do so. That the Legislature has passed a law that unconstitutionally infringes upon the right to privacy that the people of Montana have reserved to themselves in the Montana Constitution does not impose any duty, nor does it make the law necessarily valid.

Also, DPHHS was directed to seek an exemption for Montana, to get rid of the requirement that Montana demand SSNs to hunt and fish. DPHHS dis make such a request for an exemption, but it was a lightweight and ineffective request.

REQUEST FOR ADMISSION NO. 4: Admit that since the adoption of the requirement to provide a Social Security Number on wildlife conservation and hunting, fishing, and trapping license applications, the Montana Legislature has refused to repeal the requirements, while presented numerous bills to do so.

RESPONSE: Denied in part. The issue of SSNs to hunt and fish has been a contentious and divisive issue before the Legislature. In the 2001 Session, the House passed HB 282, to remove SSNs from hunting and fishing license applications, by a vote of 94-6. This bill was tabled in the Senate Fish and Game Committee because of pressure from Governor Martz. It should be noted that the pressure from Martz only arose when she broke her personal promise to me, and her promise to MSSA on her Candidate Questionnaire, to support getting SSNs off hunting and fishing license applications. While the Legislature has not mustered the political will to remove the SSN requirement, the legislative intent to mandate SSN collection has been far from unanimous.

REQUEST FOR ADMISSION NO. 5: Admit that § 7, Article IX of the Montana Constitution concerning the preservation of harvest heritage does not create a constitutional right to harvest wild fish and game animals.

RESPONSE: Objection, calls for legal conclusion.

REQUEST FOR ADMISSION NO. 6: For each individually named plaintiff, admit that you have provided your Social Security Number to obtain a driver's license.

RESPONSE: Denied in part. I have never willingly provided my SSN to obtain a driver's license. I have only provided my SSN under protest, and in order to maintain my essential livelihood. I believe that I have been unforgivably coerced into providing my SSN to be able to drive legally, and that such coercion violates the right to privacy the people of Montana have reserved to themselves in the Montana Constitution. Further, I have never allowed my SSN to appear on the face of my driver's license.

REQUEST FOR ADMISSION NO. 7: For each individually named plaintiff, admit that you have provided your Social Security Number to obtain credit or purchase an item or service.

RESPONSE: Denied. See answer to Interrogatory No. 6.

REQUEST FOR ADMISSION NO. 8: For each individually named plaintiff, admit that you have provided your Social Security Number to a federal government agency to obtain a benefit or participate in a program.

RESPONSE: Denied. To the best of my knowledge I have never provided my SSN to the federal government, except upon federal tax returns, and upon enlistment in the U.S. Army in 1966, hardly a government "program."

REQUEST FOR ADMISSION NO. 9: For each individually named plaintiff, admit that you have provided your Social Security Number to a state government agency to obtain a benefit or participate in a program.

RESPONSE: Denied. To the best of my knowledge I have never provided my SSN to a state government agency, except upon state income tax returns. Example: In February of 2006, I was invited to attend and did attend a two-day Shooting Range Development Grant Program Procedural Review conference hosted by FWP in Helena, Montana. At the conclusion of the conference I was invited to fill out forms necessary for the state to reimburse me for the costs of travel and lodging. Because I was unwilling to

provide my SSN, I was unable to complete the forms to the satisfaction of FWP, and I could not be reimbursed for the costs of attending the conference.

REQUEST FOR ADMISSION NO. 10: Admit that one or more members of the Montana Shooting Sports Association may have provided a Social Security Number to a state or federal agency to obtain a government service or benefit, including public assistance, food stamps, energy assistance, and child support enforcement.

RESPONSE: Unknown. MSSA respects the privacy of its members. MSSA would not inquire about this and would not have any information about this.

REQUEST FOR ADMISSION NO. 11: Admit that Defendants have provided adequate safeguards to protect the unauthorized disclosure of Plaintiffs (sic) Social Security Numbers.

RESPONSE: Denied. See the answer to Interrogatory No. 14. The entire system by which the State collects stores and uses hunters' and anglers' SSNs is riddled with security holes from beginning to end. The system is managed and staffed by people whose security status is unknown. The system has been electronically hacked by outsiders. The system has flunked every audit of security procedures in recent memory.

REQUEST FOR ADMISSION NO. 12: Admit that Plaintiffs (sic) right to privacy is not violated when providing their Social Security Number (sic) to a state government agency for a state statutorily authorized purpose, in conformity with a federal statute, in exchange for exercise of a privilege.

RESPONSE: Denied. See answers to Request for Admissions No. 5 and 12, and answers to Interrogatories No. 12 and 14.

REQUEST FOR ADMISSION NO 13.: Admit that the federal law authorizes a Social Security Number to be used in the provision of many government services.

RESPONSE: Unknown. I believe that federal law authorizes the use of SSNs for the purposes of the Social Security Administration and the Internal Revenue Service. If federal law specifically authorizes use of SSNs for other federal government programs I am not conversant with those laws. I do not believe that Congress is given the authority to

pass laws which have the effect of repealing rights that people have reserved to themselves in their state constitutions. Specifically, Congress is given no power to unilaterally amend the Montana Constitution, either directly or by implication. The Compact with the United States (Article I, M.C.) makes this clear.

REQUEST FOR ADMISSION NO 14.: Admit that thousands of Montana citizens benefit from the provision of public assistance and child support enforcement services in the State of Montana.

RESPONSE: Unknown. I have no direct knowledge of any individual who has received a benefit from child support enforcement in Montana. I have been told by persons who know more about the state budget than I do that zero percent of the federal funds given to Montana for child support enforcement go to benefit needy children in Montana - that 100% of these funds are spent on salaries, benefits and equipment within the Montana Department of Public Health and Human Services.

REQUEST FOR ADMISSION NO 15.: Admit that thousands of Montana citizens would suffer if the State lost millions of federal dollars in public assistance and child support enforcement funds.

RESPONSE: Denied. I don't know of any individual person who would suffer if the federal government actually quit sending money to the State for child support enforcement. Of course, there has been endless debate about whether the federal government actually would quit sending money for child support enforcement programs to the State if the State quit collecting SSNs on hunting and fishing licenses. Other states have gone to sufficient effort to obtain exceptions from the federal SSN mandate.

///

///

Further, the Montana Supreme Court has said that money is not an adequate reason for abridgement of a constitutional right. Great Falls Tribune Co., Inc. v. Day, 1998 MT 133, 289 M 155, 959 P2d 508, 55 St. Rep. 524 (1998). See answer to Interrogatory No. 12.

DATED this 20th day of September, 2006.

Respectfully submitted,

SULLIVAN, TABARACCI & RHOADES, P.C.

By: Jason B. Kuntz
Quentin M. Rhoades
Pro Querente

VERIFICATION

STATE OF MONTANA)
:ss.
County of _____)

GARY S. MARBUT, being first duly sworn, state as follows:

1. That he is one of the Plaintiffs in this action.

2. That he has read the foregoing and understand the contents.

3. That the matters, facts and things stated herein are true, accurate and complete.

IN WITNESS WHEREOF, I have hereunto set my hand and affixed my official seal the day and year herein above first written.

_____
Gary Marbut, Agent for MSSA and Individually

SUBSCRIBED AND SWORN TO before me this _____ day of September, 2006, by Gary S. Marbut.

_____
Printed Name:_____
Notary Public for the State of Montana
(NOTARIAL SEAL) Residing at: _____
My commission expires: _____

CERTIFICATE OF SERVICE

I hereby certify that on the 20th day of September, 2006, I served upon the following a true and correct copy of the foregoing by depositing said copy in the U.S. mail, postage prepaid, and addressed as follows:

Robert N. Lane
Special Assistant Attorney General
John F. Lynch
Special Assistant Attorney General
Montana Department of Fish, Wildlife and Parks
1420 East Sixth Avenue
P.O. Box 200701
Helena, MT 59620-0701

Amy K. Pfeifer
Special Assistant Attorney General
Montana Department of Health and Human Services
3075 N. Montana, Ste. 112
Helena, MT 59620

Sue Schwab
Legal Assistant to Quentin M. Rhoades