THE SENATE MAJORITY TASK FORCE ON THE INVASION OF PRIVACY

March 2000

Senate Majority Leader Joseph L. Bruno, Chairman

Senator Roy M. Goodman; Vice Chair
Senator James S. Alesi
Senator John J. Bonacic
Senator Hugh T. Farley
Senator Kemp Hannon
Senator John R. Kuhl
Senator George D. Maziarz
Senator Patricia K. McGee
Senator Michael F. Nozzolio; Vice Chair
Senator Michael A.L. Balboni
Senator John A. DeFrancisco
Senator Charles J. Fuschillo
Senator Carl L. Marcellino
Senator Serphin R. Maltese
Senator Mary Lou Rath
Senator Dean G. Skelos
Senator Caesar Trunzo

TABLE OF CONTENTS

EXECUTIVE SUMMARY

There is no private life which has not been determined by a wider public life.

George Eliot, English novelist

Privacy has become one of the most controversial subjects of the information economy due in part to modern technological developments that have opened up the flow of personal information at an unprecedented rate. In recent years, the United States has witnessed a proliferation of companies that specialize in data collection and sale. Many of these companies have built enormous databases of personal information such as Social Security numbers, address information, telephone numbers, driving records, court papers, marriage records, financial information, medical records and much more. In almost every instance, this information is being collected, sold, and distributed without the knowledge or consent of the individual to whom it pertains.

While there is an ongoing philosophical debate as to whether individuals have an inherent right to privacy, the Senate Majority Task Force on the Invasion of Privacy was created in February 1999, by Senate Majority Leader Joseph, L. Bruno, primarily for practical purposes. According to Senator Bruno, "There has always been an expectation by people that information relating to their personal lives, their health, their finances, and their family, is in some way shielded from unwanted and harmful intrusion—that expectation is no longer true."

This report is the result of research, meetings, surveys and hearings conducted by the Privacy Task Force and staff. The issue of privacy is so far-reaching in scope that this report cannot possibly cover all aspects of it. Instead, it attempts to provide an overview of the major issues needing immediate legislative attention.

Recommendations included in this document are aimed at balancing the growing privacy concerns of individuals against such benefits as freedom of information, the legitimate needs of businesses to certain information, and the ability of government to serve its functions. In addition, they incorporate the core principles of "Fair Information Practices" – Notice, Choice, and Access. It is believed by the Members of this Task Force that the following recommendations are realistic and operable solutions to better protect the personal information of New York State residents while not stifling New York's economic growth.

The Task Force wishes to lend its appreciation to those individuals who took the time to provide testimony during the hearings and assist in its mission. It should be noted that the abuses discussed in this document concerning the use of personal information by private sector businesses are not indicative of all such entities.

TASK FORCE RECOMMENDATIONS

Continue the Work of the Task Force

- Due to continuous technological changes and the complexity and scope of the issues involving privacy, the work of the Task Force should not cease with this report. Members and staff should continue to research and report on privacy issues as needed.

Social Security Numbers

- Prohibit private businesses, credit agencies, educational institutions, and not-for profits from including consumers'/clients' Social Security numbers with the information they share, sell, or trade for purposes unrelated to the individual's contract or transaction.

Criminal Activity

- Advance identity theft legislation to make it a crime to knowingly obtain one's personal information with the intent to use that information to obtain goods or services in another's name;
- Create a crime for the use of government documents for criminal activity; and
- Provide for the creation of a crime of surreptitious video surveillance in a private dwelling without consent.

Crime Victims

- Prohibit the publication or broadcasting of information identifying a sexual offense victim;
- Provide for the confidentiality of the address and telephone number of a victim or witness to a crime;
- Prohibit the disclosure of felony crime scene photographs, except for specified purposes;
- Identity Theft Victims – Provide for an "expedited" process whereby identity theft victims can petition a court or administrative body to make a finding and issue an order in cases where evidence of identity theft can be clearly demonstrated, thereby facilitating efforts to restore the victim's credit history;
- Develop initiatives to curtail the abusive practices of collection agencies, particularly when actions are directed at identity theft victims;
- Increase civil penalties for credit reporting agencies' willful noncompliance with the resolution of identity theft matters;
- Identity Theft/Consumer Fraud Assistance Board – Establish an Identity Theft/Consumer Fraud Assistance Board under the auspices of the Consumer Protection Board to provide assistance to identity theft victims; and
- Identity Theft/Consumer Fraud Assistance Fund – Establish an Identity Theft/Consumer Fraud Assistance Fund for victim assistance and investigations.

State Agency Records

- Direct agencies to have safeguards in place to prevent the release of personal information by employees for purposes other than its original intention (e.g. violations of law through the use of technological advances); and
- Restrict State agency use of personal information for marketing purposes.

Motor Vehicle Records

- Prohibit the sale of DMV's registration and title information;
- Mandate greater oversight by DMV over "requestor" use and requestor resale/redisclosure to third parties by requiring DMV to undertake compliance audits and file annual reports with the Legislature;
- Increase penalties for improper disclosure by DMV, and other parties; and
- Provide DMV with sufficient means to impose appropriate sanctions including the ability to immediately suspend or revoke requestor privileges to obtain information.

Insurers

- Establish standards for the collection, use and disclosure of information by health, property/casualty, life and disability insurers, insurance institutions, and agents or insurance-support organizations.

E-ZPass Records

- Prohibit E-ZPass account information from being released to any person or authority other than the account holder, with exceptions for law enforcement or court order.

Inmate Access to Information

- Prohibit inmates from accessing personal information either through mail or via computerized databases when working on State contracts; and
- Amend the Civil Rights Law and/or the Freedom of Information Law to restrict inmate access to certain personal information.

Internet, Data Dealers

- Provide individuals with the right to "opt-out" of having their personal information sold or shared by data dealers;
- Require companies that collect personal information to allow "data subjects" to view personal information that pertains to them;
- Advance anti-spamming legislation to reduce the transmission of unsolicited e-mail; and
- Adopt Internet privacy policies for the Legislature as well as for each agency prohibiting the sale of any personal information gathered as a result of comments/questions submitted by web site visitors.

Financial Institutions

- Privacy Policy – Require financial institutions to have a privacy policy for the use of customer information and require them to make it available to customers;
- Notification – Require financial institutions to notify customers at least annually that their personal information may be used for marketing purposes;
- Opt-out – Provide customers the ability to opt-out of having their personal information sold or leased for marketing purposes; and
- Customer Access – Give customers the right to review the information kept about them and the ability to correct inaccuracies.

Children/Student records

- Direct school districts, colleges and universities to have in place, policies concerning the release of students' personal information and make such policies available; and
- Prohibit the use by public or private schools and colleges of student Social Security numbers as student identification numbers or for any student identification purpose except for the employment of a student, financial aid or to adhere to state and federal statutes and regulations.

Credit Agencies

- Instant Credit Offers – Require at least 2 forms of identification for instant credit, one must include photo ID and one must include the applicant's address;
- Credit Approval/Activation Procedures and Mailing Lists – Require written credit offers and advertisements for credit mailed to a consumer to contain instructions for the removal of the consumer's name from the mailing list;
- Require mail offer issuers to only approve credit applications containing an address that matches the address in the CRA's file. Any change of address must be separately verified;
- Provide that issuers require automated credit card activation from the consumer's home phone of record (business phone, if a corporate card is issued).
- Annual Free Credit Report – Require CRAs to annually provide one free copy of a consumer's credit report, upon request;
- Consumer Bill of Rights – Direct CRAs to include a summary of "consumer rights" in each free consumer credit report;
- Third Party Disclosure – Require CRAs to include a list of each third party that has requested information on the consumer, during the preceding 12 months, for any purpose, including for inclusion on marketing lists;
- Toll-Free Number – Direct CRAs to provide a toll-free number and address a consumer may use to remove his or her name from mailing lists offering credit. Further require that such information be included in any credit report provided to the consumer (free or otherwise);
- Sale of Personal Information – Make it illegal for CRAs and card issuers to sell consumers' credit card numbers for non-authorized purposes, including marketing purposes;

Businesses

- Privacy Policy – Require private businesses that collect and distribute personal information, to have a privacy policy for the use of such information and require them to make it available to customers;
- Notification – Require such entities to notify consumers as to whether their personal information is being sold or shared;
- Opt-out – Allow customers/consumers the right to opt-out of having their personal information sold or leased for marketing purposes; and
- Customer Access – Give customers the right to review the information kept about them and the ability to correct inaccuracies.

Telemarketers

- Create a state "do-not-call" list;
- Require telemarketers to be bonded and registered with the Department of State;
- Create standards of conduct which prohibit abuses (e.g., harassment, failure to honor do-not-call requests) and establish corresponding civil and criminal fines;
- Prohibit telemarketers from accessing customers' checking, savings, and other accounts without authorization;
- Prohibit courier pick-up for advance payments; and
- Establish specified record-keeping requirements.

Medical Records

- Advance legislation to prohibit insurers, pharmacies, hospitals, public and private health clinics, health care providers, health care practitioners, and health care facilities from sharing or selling personally identifying medical/health information for any purpose not directly related to the patient's/client's treatment or account maintenance without his or her consent unless otherwise required by federal or state statute.

BACKGROUND

Historically, the United States has been a relatively open society in the area of information practices. Federal and state laws have played a role in establishing this openness.[1] The U.S. constitution does not make mention of "privacy" nor does it generally constrain actions by private parties. Privacy rights have generally been limited to constitutional provisions governing search and seizure, due process, freedom of the press, and voting rights.[2] American laws have, for the most part, been used to limit the actions of government rather than behavior between citizens. This regulatory philosophy has favored the free flow of information in our society. However, it is doubtful that at the inception of this nation, its constitutional framers imagined a society where individuals' personal information could be accessed as easily as it is today.

Since the Privacy Act of 1974, intrusions on personal privacy have increased exponentially, yet statutory protections aimed at preserving individuals' privacy are not much greater than they were 26 years ago. This lack of protections has allowed fervent privacy intruders, driven by profit and technological advances, to circumvent our antiquated privacy laws.[3] Not to say that government has enacted no laws concerning the use of personal information. However, in almost every instance, such enactments were swift reactions to very specific problems (sometimes scandals) which has led to a patchwork of often limited and ineffective privacy protection laws.

The word privacy conjures up different thoughts for different people. It can relate to privacy invasions by the tabloids, searches and seizures, cameras in the courtroom or Peeping Toms. Each of us reacts differently to invasions of our privacy, judged in part by the standards we hold and by the relationship of those to whom we open up our lives. Philosophers, psychologists, sociologists, journalists, legal scholars, business professionals and consumers attach a different meaning to privacy.[4] The definition of privacy can be traced back to legal scholars Samuel D. Warren and Louis D. Brandeis. They defined privacy as "the general right to be left alone" in an 1890 *Harvard Law Review* article.[5] This Task Force has focused primarily on the newest and fastest growing privacy concern – information privacy. We will define "information privacy" as the ability of an individual to control or at least significantly influence the handling of data concerning him or herself.

Two prevalent themes emanate from discussions of information privacy – accessibility and control. Access has to do with the ability of others to obtain your personal information and know your purchasing behaviors, preferences, and products purchased. Control involves your right to prevent the disclosure of personal information or the right to know which information is kept on you and how it is used. The Task Force has made recommendations to reduce unwanted accessibility of personal information by third parties and to provide ways to give individuals greater control over their personal information.

FAIR INFORMATION PRACTICES

The Code of Fair Information Practices was the central contribution of the HEW (U.S. Department of Health, Education and Welfare) Advisory Committee on Automated Data Systems established in 1972. Its broadly recognized principles were designed to ensure that individuals are able to "determine for themselves when, how, and to what extent information about them is shared." The Code was never enacted into law, but remains a sound and enduring baseline for evaluating the information handling practices of businesses and government.

The Code of Fair Information Practices is based on five principles:

1. There must be no personal data record-keeping systems whose very existence is secret.

2. There must be a way for a person to find out what information about the person is in a record and how it is used.

3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.

4. There must be a way for a person to correct or amend a record of identifiable information about the person.

5. Any organization creating, maintaining, using, or disseminating records of identifiable personal data must ensure the reliability of the data for their intended use and must take precautions to prevent misuses of the data.

PRIVACY BY THE NUMBERS – SOME STATISTICS[6]

Chance that a U.S. citizen believes his or her privacy has been violated: **1 in 4**

Minimum cost of obtaining an e-mail address for marketing purposes: **1 cent**

Number of pieces of junk e-mail delivered each day on America Online: **9 million**

Number of pieces of junk mail delivered each day by the U.S. Postal Service: **600 million**

Estimated weight of U.S. junk mail delivered each year, in tons: **4 million**

Percentage of commercial Web sites that collect personal information: **92**

Percentage of commercial sites that have a comprehensive privacy policy: **2**

Percentage of people who lie when asked to provide personal information over the Web: **40**

Estimated corporate losses from computer crime in 1997: **$136 million**

Annual losses from credit-card fraud: **$700 million**

Chance that your credit report contains a serious factual error: **3 in 10**

Number of state and federal wiretaps issued in 1997: **1,186**

Number of phone conversations employers eavesdrop on each year: **400 million**

Increase in the number of U.S. workers under electronic surveillance since 1991: **275 percent**

Number of insurance companies that access the Medical Information Bureau database: **750**

Number of federal laws that protect the privacy of medical records: **0**

Number of federal laws that protect the privacy of video rentals: **1**

Number of privacy bills introduced in state legislatures in 1997: **over 8,500**

Number of times the word privacy appears in the U.S. Constitution: **0**

Source: PC World Magazine, September, 1998.

PUBLIC ATTITUDES ABOUT THE PRIVACY OF INFORMATION

I've never looked through a keyhole without finding someone was looking back.

"Judy Garland (1967) US actress, singer"

Privacy is such a personal issue that peoples' attitudes about it differ greatly. The willingness to provide access to personal information is often contingent on the reward for doing so. Such rewards often take the form of additional savings, coupons, and rebates. Since personal information has value, if you choose to withhold it, you may deny yourself certain advantages.[7] Generally, people are willing to provide some personal information to the party they are "doing business" with–it is the release of that information to third parties that greatly concerns them. Marketers contend that people enjoy receiving unsolicited information since it makes them more aware of products and services that are available to them. However, results from numerous recent national polls have concluded that people want to retain some control over who knows what about them. One of the most compelling of the polls on privacy came from a Wall Street Journal-NBC poll in the Fall of 1999. Americans were asked what they feared most in the coming century. Answers included terrorism, global warming, overpopulation and numerous other horrible things. The answer that came in highest (29% of all respondents) was the loss of privacy—no other topic rose above 23%.[8]

1996 DIRECT Poll[9]

A survey conducted in 1996 for a prominent direct marketing magazine revealed that:

- 83% of survey participants said there should be a law requiring an "opt-in" procedure to be included on mailing lists;
- 78% are in favor of such a law even if it means they would not receive new mailings;
- 58% want to outlaw altogether the collection of Social Security numbers; and
- 58% said they do not even look at their direct mail before throwing it away.

1997 Money Magazine Poll[10]

- 74% of the public are somewhat or very concerned about threats to their privacy;
- 29% have experienced a serious invasion of their financial or medical information; and
- 65% are more worried about privacy invasion than they were 5 years ago.

Public Agenda Online Poll[11]

How concerned are you about the theft of your personal identity numbers, such as Social Security, cell phone, phone card, or bank account numbers?

- 57% very concerned;
- 29% somewhat concerned;
- 10% not too concerned;
- 3% not concerned;
- 1% don't know.

Do concerns about the security of these numbers ever stop you from making purchases over the phone or via the Internet?

- 66% yes;
- 30% no;
- 4% don't know.

1999 IBM Consumer Privacy Survey[12]

A December 1999 international privacy survey by IBM found that:

- 94% of consumer respondents in the United States, 78% in the United Kingdom, and 72% in Germany said they think personal information is vulnerable to misuse; and
- 78% of American consumer respondents, 58% of British consumers, and 52% of German consumers claim they have refused to provide requested data to a business because they believe it is too personal.

1998 AARP Survey[13]

AARP's Public Policy Institute sponsored a national telephone survey of AARP members to measure their awareness of privacy attitudes and ascertain their attitudes toward current practices of selling and sharing customer information. Some major findings from the survey include the following:

- A majority of respondents believed that businesses are allowed to gather personal information about consumers without their permission, including whether they pay their bills on time (82%); the long distance carrier they use (76%); their Social Security numbers (68%); their medical histories (60%); and the amount of money in their bank accounts (55%);

- 78% of the respondents disagreed with the following statement: "current federal and state laws are strong enough to protect your personal privacy from businesses that collect information about consumers";

- 87% of respondents said it would bother them if personal information were sold by businesses, government agencies or Web sites to other businesses;

- 81% of respondents opposed the internal sharing of customers' personal and financial information by corporate affiliates; and

- 42% of respondents indicated they "didn't know" who they would turn to for assistance if a company was inappropriately sharing or selling their personal information.

SOME WAYS PERSONAL INFORMATION MAY BE OBTAINED*

If You've	You Gave Up This Information	Here Is Where it Ends Up
Registered to vote	Your name, address, birth date, birth place, occupation, political affiliation, and signature	Voter registration records are open to public inspection in most states and part of nationwide commercial databases.
Bought a house	Spouse's name, address, purchase price, loan amount, down payment, property description	Property tax information, deeds, and trust deeds are open for public inspection, available at title companies, and stored on public and commercial databases.
Had a baby	Baby's name and date of birth, parent's names, addresses, jobs; medical information	Most states do not seal birth records, which is why new parents receive so much junk mail for baby products.
Own stock in a company	Your name, the number of shares you own, your address if you are a corporate officer	The Securities and Exchange Commission makes public the names of anyone owning 15% or more of the stock shares in a publicly held firm.
Given more than $50 to a campaign	Your name, title, address, employer, and amount of contribution	Campaign disclosure laws generally make contributions public at all levels of government.
Had your dog vaccinated for rabies	Your name, address, phone number, animal's name, age, breed	Many states require veterinarians to report information to the animal regulation department, which regularly sells the information to commercial firms.
Taken out a permit for a yard sale	Your name, address, sometimes phone number, date of sale, signature	Such records are generally available for inspection.
Paid a fine for an overdue library book	Your name, address, phone number, book titles, due date, return date, fine paid	Librarians have fought to keep patrons' information private, but when a law is violated, the records are almost always public.
Received a parking ticket	Your name, address, vehicle make, license number, date of violation, place of violation, fine	Copies of citations are usually available at the police department or local court, sometimes the department of motor vehicles is informed.
Participated in a phone survey	Aside from your opinions, your name, address, phone number, age, income level, and more	The data could be sold to advertisers, mail-order companies, commercial businesses, or government agencies.
Mailed in a warranty card	Your name, address, phone number, age range, income range, interests	Warranty cards are nothing more than marketing surveys, companies may hold the information or sell it.
Entered a contest or sweepstakes	Your name, address, phone number, and possibly more marketing information	The information will be distributed to numerous other companies.
Used your ATM card for any purchase	Your name, bank, account number, and balance, what you purchased	No one knows how far grocery stores, restaurants, and other retailers will go with your information. Knowing who you are and what you buy is available to marketers.
Rented a movie	Your name, address, phone number, credit-card number, movie preferences	Though they can't disclose what movies you've rented, video stores can share your contact information and general preferences.
Subscribed to a magazine	Your name, address, phone number, and at least one interest – the magazine topic	Magazines sell their mailing lists to generate revenue.
Source: PC World Magazine, September, 1998.		

* May vary by state and locality

THE SOCIAL SECURITY NUMBER – A UNIVERSAL IDENTIFIER

The Social Security number (SSN) was created in 1936 as a means of tracking workers' earnings and eligibility for Social Security benefits. Today, the SSN is used for numerous purposes, some legal and some illegal.[14] The uniqueness and broad applicability of the SSN have made it the identifier of choice for government agencies as well as private businesses. A number of federal laws require the use of the SSN for government benefit eligibility, taxation, Commercial Driver's Licensing, child support and more. Likewise, federal laws do not prohibit its use by government or prohibit private businesses from requesting it and using it for purposes unrelated to one's transaction or contract.

The federal Privacy Act of 1974 (P.L. 93-579) Section 7, states that it shall be unlawful for any federal, state or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security number. These provisions do not apply to "any disclosure which is required by federal statute, or the disclosure of a Social Security number to any federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. Any federal, state, or local government agency which requests an individual to disclose his Social Security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.

The SSN can be the key to considerable amounts of personal information, including tax information, credit information, school records, and medical records. SSNs are bought, sold, and shared every day. Information brokers or "data dealers" as they are commonly referred to, build tremendous databases of personal information often including peoples' SSNs. Data dealers prefer to buy information attached to one's SSN because it is more likely to produce fairly accurate information.

In recent years, a number of bills have been introduced in Congress that would better protect an individual's SSN by restricting its use and sale (for bill numbers, refer to the section on federal measures). New York State General Business Law, Section 518-a, prohibits sellers/merchants from recording an individual's SSN on a check during a transaction.

CRIMINAL ACTIVITY

"Gentlemen, do not read each other's mail."

Henry Lewis Stimson (1948) US government official

THE GROWING CRIME OF IDENTITY THEFT

Identity theft is one of the fastest growing crimes in the nation, impacting about 400,000 victims each year. Identity thieves range from street pickpockets to sophisticated computer hackers. A thief need only obtain a Social Security number or a blank pre-approved credit application to commit this type of fraud. While innocent victims may not be responsible for paying the bills the thieves run up, the violated person may spend years and thousands of dollars trying to clear his or her name and once again obtain credit.

Identity theft is growing for several reasons. One reason may be the fact that it is relatively easy to obtain credit.[15] There is considerable competition among creditors for customers sometimes leading to inadequate checks of identity prior to the granting of credit. Pre-approved credit offers are very popular with identity thieves since the initial screening is already done. Another incentive for thieves to choose this crime is the availability of personal information (particularly Social Security numbers) needed to commit the acts. Some gangs have found identity theft to be more attractive than the traditional face-to-face crimes since there is less risk of getting caught due to law enforcement resources concentrated on combating violent crimes. In addition, when thieves are caught, the penalties are less severe than for crimes like burglary or robbery.

Skilled identity thieves use a variety of methods to obtain the necessary personal information to assume one's identity. The following table highlights some of the ways identity thieves can obtain someone's personal information and how they can use it.

How Identity Thieves Get Your Personal Information	How Identity Thieves Use Your Personal Information
They steal wallets and purses containing your identification and credit and bank cards.	They call your credit card issuer and ask to change the mailing address. Then they run up debt in your name.
They steal your mail, including your bank and credit card statements, pre-approved credit offers, telephone calling cards and tax information.	They need little more than your SSN to open new credit cards – of course the bills never get paid.
They complete a change of address form and have your mail sent to another location.	They establish phone or wireless service in your name.
They rummage through trash for bills and other personal data. This practice is called "dumpster diving."	They open a bank account in your name and write bad checks.
They obtain your credit report by posing as someone who has a "permissible" purpose for viewing it.	They file for bankruptcy under your name to avoid paying debts they have incurred in your name, or to avoid eviction.
They get your business or personnel records at work.	
They find personal information in your home.	They counterfeit checks or debit cards and drain your bank account.
They use personal information you share on the Internet.	
They buy your personal information from store employees, Internet data sellers or a number of other sources.	They buy or lease cars by taking out auto loans in your name.
Adapted from ID Theft: When Bad Things Happen To Your Good Name. FTC, February 2000.	

In 1998, Congress passed the Identity Theft and Assumption Deterrence Act (codified in part 18 U.S.C. Section 1028), making it unlawful for anyone to knowingly transfer or use, without lawful authority, another person's identification with the intent to commit an unlawful act. The new law establishes criminal penalties for identity theft offenses and provides for restitution for victims. A number of states have enacted identity theft legislation. While most recent statutory changes involve establishing penalties for specific offenses, some aim to provide consumers with greater control over their credit information in hopes of preventing such acts.

STATE IDENTITY THEFT LAWS	
Arizona	Ariz. Rev. Stat. Sect. 13-2708
Arkansas	Ark. Code Ann. Sect. 5-37-227
California	Cal. Penal code Sect. 530.5
Connecticut	1999 Conn. Acts 99
Georgia	Ga. Code Ann. Sect. 121
Idaho	Idaho Code Sect. 28-3126
Illinois	720 ILCS 5/16/G
Iowa	Iowa Code Sect. 715A8
Kansas	Kan. State Ann. Sect. 21-4108
Maryland	Md. Ann. Code art. 27 sect. 231
Massachusetts	Mass. Gen. Laws ch. 266 Sect.37B
Mississippi	Miss. Code Ann. Sect. 97-19-85
Missouri	Mo. Rev. State Sect. Sect. 570.223
New Jersey	N.J. State Ann. Sect. 2C:21-17
North Dakota	N.D.C.C. Sect. 12.1-23-11
Ohio	Ohio Rev. Code Ann. 2913
Oklahoma	Okla. Stat. Tit. 21, Sect. 1533.1
Tennessee	Tenn. Code Ann. Sect. 39-14-150
Texas	Tex. Penal Code Sect. 32-51
Washington	Wash. Rev. Code Sect. 9.35
West Virginia	W. Va. Code Sect. 61-3-54
Wisconsin	Wis. Stat. Sect. 943.201
Source: ID Theft: When Bad Things Happen To Your Good Name. FTC February 2000.	

If you believe you have been a victim of identity theft, you should file a complaint with the Federal Trade Commission by contacting the FTC's toll-free Identity Theft Hotline at 1-877-IDTHEFT (438-4338); by mail: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580; or online: www.consumer.gov/idtheft
In addition, contact the 3 credit bureaus (refer to the section on credit agencies for contact information), your bank, credit card issuing companies or other lenders you deal with, and the company you purchase checks from. Three of the check verification companies that accept reports of check fraud directly from consumers are:[16] Telecheck: 1-800-710-9898, International Check Services: 1-800-631-9656, Equifax: 1-800-437-5120.

A Few Ways to Limit Circulation of Your Personal Information According to the FTC

Pre-Screened Credit Offers

If you receive pre-screened credit card offers in the mail (namely, those based upon your credit data), but don't tear them up after you decide you don't want to accept the offer, identity thieves may retrieve the offers for their own use without your knowledge. To opt out of receiving pre-screened credit card offers, call: 1-888-5-OPTOUT (1-888-567-8688). The three major credit bureaus use the same toll-free number to let consumers choose not to receive pre-screened credit offers.

Marketing Lists

To have your name removed from unsolicited preapproved mail offers from the three major credit bureaus call the MCI “opt-out” toll-free number at 1-(888) 567-8688.

Departments of Motor Vehicles

All the personal information on a driver’s license and more is on file with the state Department of Motor Vehicles (DMV). A state DMV may distribute your personal information for law enforcement, driver safety or insurance underwriting purposes, but you have the right to choose not to have the DMV distribute your personal information for other purposes, including for direct marketing. The New York State DMV allows drivers to “opt-out” of having their personal information sold. (For more information, refer to the section on motor vehicle records.)

Direct Marketers

The Direct Marketing Association's (DMA) Mail, E-mail and Telephone Preference Services allow consumers to opt-out of direct mail marketing, e-mail marketing and/or telemarketing solicitations from many national companies. Because your name will not be on their lists, it also means that these companies can't rent or sell your name to other companies. To remove your name from many national direct mail lists and direct telephone lists, refer to Attachment A or visit www.the-dma.org

USE OF GOVERNMENT DOCUMENTS FOR CRIMINAL ACTIVITY

The Freedom of Information Law (FOIL) is based on the idea that "a free society is maintained when government is responsive and responsible to the public, and when the public is aware of governmental actions." It was this idea of open access to government documents that has, unfortunately, come under abuse by convicts and others with questionable and/or harmful motives. Recently, there has been an increase in instances of unscrupulous individuals using FOIL to gain access to personal data on unsuspecting citizens.

VIDEO SURVEILLANCE

Currently, there are no statutory provisions that protect individuals from being observed in what should be considered their private residence. The General Business Law prohibits businesses from engaging in surreptitious surveillance, but is silent on the matter of private dwellings. At this time, an individual would have no recourse if videotaped unknowingly in his or her own home or in a neighbor’s. A recent 2020 news special revealed how one homeowner videotaped neighbors while they changed clothes in his bathroom.

CRIME VICTIMS

The crime of a sexual assault against an individual is one of the most personal offenses that can be committed. The New York State Coalition Against Sexual Assault estimates that 1 of 3 women are sexually assaulted in their lifetimes. A number of statutes have been enacted in recent years to strengthen the penalties for sexual offenses and to expand protections for the public. Unfortunately, there are still issues of protection that need to be addressed. One issue is the need for a victim's anonymity. Anonymity from the public eye would assist a victim while on the road to recovering from an offense. The ability to remain anonymous may be a determining factor for a rape victim to file a police report and pursue a legal course of action against the offender.

The recent trend of acquiring crime-scene photos for posting on the Internet or to be used by convicted felons for bragging rights in unconscionable. One of the most notorious cases of such abuse is exemplified in the recent State Supreme Court case in which a state judge ordered Buffalo officials to provide convicted killer Rodney James with graphic crime scene photos of his victim. Clearly, the harm such disclosure causes to the victims and their families, especially given the lack of a legal reason for the release of such photos, calls for some degree of privacy protections to be put in place.

Victims of identity theft often face aggressive collection agencies and creditors demanding they pay the bills incurred with their name. There have even been instances where bounty hunters confronted identity theft victims trying to obtain stolen merchandise. These experiences can be extremely frightening for individuals who in some cases, are unaware they have been victimized. Currently, there is insufficient support for identity theft victims, particularly with regard to the restoration of their credit history. A state board with expertise in identity crimes could be useful in providing assistance to victims of the fastest growing crime in America.

GOVERNMENT USE OF INFORMATION

"We are rapidly entering the age of no privacy, where everyone is open to surveillance at all times; where there are no secrets from government." [17]

Justice William O. Douglas (1966)

Information is power, so it is not surprising that governments have kept pace with the private sector in the race for information. Government collects a great deal of information from people today. Much of the information is needed for public purposes such as tracking benefit claimants, providing health care services and fighting crime.[18] Unfortunately, some of this personal information is being used for purposes for which it was not originally intended. A significant portion of personal information that enters the databases of data dealers is obtained unknowingly from consumers when they apply for a driver's license or fill out another type of government form. With advances in technology, it is plausible that in the near future all government records will be in electronic form, making it necessary to have safeguards in place that ensure the privacy of the individuals to whom the information pertains.

Access to certain public records is not a recent development. Access to tax assessment records has historically served the purpose of allowing the property owner to ascertain if he or she is being treated fairly by government. Motor vehicle records have historically served numerous purposes, including law enforcement, vehicle recall, auto insurance, child custody and child support. Most state, federal, and local agencies keep public records for legitimate governmental purposes. The ability to use public records to invade someone's privacy has been a concern of legislators since the 1989 murder of 21-year-old television actress Rebecca Schaeffer, who was killed by a stalker who obtained her address from the California Department of Motor Vehicles records.[19] Seventeen states now prohibit the sale of DMV information.

FREEDOM OF INFORMATION LAWS

The Freedom of Information Act (FOIA), which can be found in Title 5 of the United States Code, Section 552, was enacted in 1966 and provides that any person has the right to request access of federal agency records or information. All agencies of the United States government are required to disclose records upon receiving a written request except for those records that are specifically exempted from disclosure under FOIA. The federal FOIA does not, however, provide access to records held by state or local government agencies, or by private businesses or individuals. All states have their own statutes governing public access to state and local records.

New York's original Freedom of Information Law (FOIL) was enacted in 1974 (Chapter 578, L.1974) and underwent revision in 1977 (Chapter 933, L.1977) (Public Officers Law, Article 6). The 1974 law created the Committee on Public Access to Records (COPAR) to oversee the implementation of the law. In 1983, COPAR was changed to the Committee on Open Government (Chapter 80, L. 1983). The Committee falls under the jurisdiction of the Department of State and furnishes advice to agencies on implementing the law. The law directs that each agency make available all records for public inspection and copying. Each State agency

has a designated person or office that processes FOIL requests. The term "agency" includes all units of State and local government. Courts are not subject to the law. The term "record" means any information kept, held, filed, produced or reproduced by, with or for any agency or the State Legislature.

Agencies may deny access to records that:

- are specifically exempted from disclosure by federal or State statute;
- if disclosed would constitute an unwarranted invasion of personal privacy (employment, medical or credit histories; sale or release of lists of names and addresses if they would be used for commercial or fund-raising purposes; disclosure of personal information that would create an undue personal or economic hardship to the subject party and not relevant to agency work); or
- were reported in confidence to an agency and not relevant to agency work.

Agencies cannot release information that is prohibited under Section 96 of the Public Officers Law (the Personal Privacy Protection Law).

THE NEW YORK STATE PERSONAL PRIVACY PROTECTION LAW

Currently, New York State agencies are governed by the provisions of Article 6-A of the Public Officers Law with respect to the release, disclosure, and dissemination of personal information. Section 96 specifies that an agency may disclose personal information if it is:

- pursuant to a written request by or the voluntary written consent of the data subject;
- to those officers and employees of, and to those who contract with, the agency that maintains the record if the disclosure is necessary to the official duties of the agency;
- subject to Article 6 of the Public Officers Law (the Freedom of Information Law), unless release of such records would constitute an invasion of personal privacy as defined by Section 89;
- to another governmental unit if the information is necessary for meeting statutory requirements;
- for routine agency use;
- for purposes specifically authorized by state or federal statute;
- to the Bureau of the Census;
- to a person who has assured the agency that the information will be used solely for statistical or research purposes, but only if it is to be transferred in a form that does not reveal the identity of any data subject;
- pursuant to a showing of compelling circumstances affecting the health and safety of a data subject, if upon such disclosure notification is transmitted to the data subject;
- to the State Archives as a record that has historical value;
- pursuant to a court order;
- for inclusion in a public safety agency record or to a governmental unit which performs criminal law enforcement for such purpose;

- pursuant to a search warrant; or
- to officers or employees of another agency if the record sought to be disclosed is necessary for the receiving agency to comply with the mandate of an executive order, but only if the records are to be used for statistical research, evaluation or reporting and are not used in making any determination about the data subject.

Nothing in this section shall require disclosure of:

- personal information which is otherwise prohibited by law from being disclosed;
- patient records concerning mental disability or medical records where the disclosure is not otherwise required by law;
- personal information pertaining to the incarceration of an inmate at a state correctional facility which is evaluative in nature or which, if disclosed, could endanger the life or safety of any person, unless the disclosure is otherwise permitted by law; or
- attorneys' work product or material prepared for litigation before judicial or administrative tribunals.

MOTOR VEHICLE RECORDS AND THE DRIVER'S PRIVACY PROTECTION ACT

In 1994, Congress enacted the Driver's Privacy Protection Act (DPPA) (18 U.S.C. Section 2721) to remedy what was perceived as a problem of national concern about the release of personal information contained in motor vehicle records. States were given 3 years to comply with the law by implementing procedures to restrict public access to motor vehicle records. The law placed some restrictions on the release of personal information. Personal information, as defined by the DPPA, includes a person's name, address not including the zip code, photograph, telephone number, Social Security number, driver's license identification number, medical or disability information, and date of birth.

The DPPA allows individuals or companies to obtain information for the following uses:

- for government purposes, including court use and law enforcement;
- in the normal course of business activity by a legitimate business to verify personal information submitted by the person;
- in connection with any civil, criminal, administrative, or arbitrational proceeding;
- in research activities and statistical reports, provided that the personal information is not published, re-released, or used to contact individuals;
- by any insurer or insurance support organization;
- in providing notice to owners of towed vehicles;
- by a licensed private investigator or security service;
- by an employer to obtain or verify information on a commercial driver's license;
- in connection with private toll transportation facilities;
- in response to requests for individual records if the state motor vehicle agency has provided clear and conspicuous notice on forms for issuance or renewal of a driver's license or identification card that the personal information may be disclosed to anyone, and that the agency provides the person an opportunity to opt out of having his/her information disclosed;

- in connection with bulk distribution for surveys, marketing, or solicitation if a person has not opted out;
- by a requestor, if there is written consent from the individual to whom the information pertains; and
- specifically authorized by state law, if such use is related to the operation of a motor vehicle or public safety.

The DPPA restricts the redisclosure and/or resale of personal information. An authorized recipient may redisclose the personal information obtained from a state DMV only to another permitted user, for a permitted use.

There have been several recent constitutional challenges to the DPPA with South Carolina becoming the first state to take such action. A federal judge in South Carolina declared the law unconstitutional (C.A. No.3: 96-3476-19) and blocked the enforcement of the DPPA in that state. The judge declared that Congress wrongly directed states to enforce federal policy by requiring the states to regulate the dissemination and use of records. The U.S. Department of Justice filed an appeal of the South Carolina ruling and this year, the Supreme Court upheld the constitutionality of the DPPA.

DPPA Implementation in New York

Registration Information

Currently the State Department of Motor Vehicles sells the following information: title/vehicle registrations for snowmobiles, boats, ATVs and motorcycles and emissions inspection information to the highest bidder(s) unless the motorist checks a small box prohibiting the release of this information (VTL 202(4)). This "opt-out" box is found on registration and registration renewal forms (Refer to Attachment B for DMV Vehicle Registration/Title Application)

DMV, in the most recently awarded contracts is receiving over a two-year period, approximately $3.6 million dollars. The successful bidder(s) may resell/redisclose this information which consists of : name and address of the owner of the vehicle and the make, model, year, weight, body style, number of passengers and cylinders, fuel, license number, type of registration and transaction, validation and expiration date and vehicle identification number of vehicle.

Drivers License Information

The Department takes the position that information on the driver license is private unless the "requestor" meets a "permissible use" under the guidelines of the federal DPPA. These permitted users are insurance companies, rental car agencies, private investigators, etc. Information released consists of: name, address, driver information and driving record. SSN, photo, and telephone number are not released except for law enforcement purposes and pursuant to judicial subpoena. The sale/lease of license information provides the Agency with considerable revenue. A large number of requestors (insurance industry, passenger car rental companies, private investigators, information retrieval services) provide this substantial stream

of revenue. Those who use the information frequently may apply for "dial-in-access" to DMV databases.

An authorized recipient may redisclose the personal information obtained from DMV to a third party only if the recipient is a permitted user for a permitted use. The law requires that a record of such redisclosure, including the identity of the party to whom the information was disclosed and the permitted purpose for which it was used, be retained for 5 years.

NEW YORK STATE E-ZPASS RECORDS

New York State is the nation's leader in the development of Electronic Toll Collection. In 1993, the New York State Thruway Authority introduced E-ZPass in order to relieve traffic congestion at the toll booths. There are currently 2.7 million E-ZPass tags distributed in New York State, with the number increasing. The electronic tags leave a trail that can be traced. While E-ZPass claims that the information is not released to anyone but the account holder, others have accessed them. Such information is valuable to private investigators, stalkers, divorce attorneys and anyone who wants to track someone's driving patterns and whereabouts. With the future expansion of E-ZPass to include airport parking, purchases, and other interstate tolls, there is even greater opportunity for personal information to find its way into the wrong hands.

INMATE LABOR & ACCESS TO RECORDS

Historically, inmates have performed government work while serving time in order to develop skills and keep busy. However, there have been numerous reports in some states about prisoners accessing personal information and using it to harass innocent citizens. A recent congressional report found that inmates working on government contracts involving telephone contact have used credit card numbers and other personal information to commit fraud and harass customers.[20] Prisons in at least 20 states have contracted with local, state, and federal governments to handle records that may include individuals' names, addresses, phone numbers, birth dates, Social Security numbers, and credit card numbers.[21]

INFORMATION IN THE PRIVATE SECTOR

"Privacy is like clean air. At one time there was plenty of it. Now it's almost gone."[22]

Kevin Murray, Security Expert

Restrictions on private sector access and use of personal information has been relatively nonexistent, instead relying on industry self-regulation.[23] A number of private as well as public entities compile personal data about individuals. Direct marketers receive personal information from a number of sources including: colleges and universities, credit card companies, department stores, hospitals, and government agencies. In addition, a number of other affiliations such as book clubs, newspaper companies, car dealers, and not-for-profits release information about their customers. Grocery stores use special customer cards to track how much people spend and what types of products they are purchasing. While some businesses have privacy policies explaining their use of customer buying habit information, others sell the information to direct marketing companies for solicitation purposes without the customer's knowledge or consent.

THE FLOW OF ELECTRONIC INFORMATION

According to a recent survey, 70 million adults, or one-third of Americans over age 16, use the Internet.[24] The recent acquisition of Time Warner by Internet giant America Online for $165 billion is evidence of the growing influence of Internet services. America Online will gain access to Time Warner's entertainment and information empire and its 22 million paying subscribers.[25] Every day millions of people surf the Internet posting messages to newsgroups, chatting with friends, and browsing web sites, unaware that they leave traces of where they have been and perhaps what they have said. According to PC World, each piece of electronic correspondence can be seen by millions of Internet users for many years to come. Virtually all online services offer some sort of "private" activity which allows subscribers to send personal e-mail messages to others. While the federal Electronic Communications Privacy Act (ECPA) makes it unlawful for anyone to read or disclose the contents of an electronic communication (18 USC § 2511), there are certain exceptions to the law, such as if the user provides consent when signing up for service.

In June1998, the Federal Trade Commission issued a report claiming that web sites are not doing enough to protect surfers' privacy. The FTC surveyed 1,400 American Internet sites and found that only 2% had posted a privacy policy in line with that advocated by the Commission.[26] Instead of promulgating new regulations, the Commerce Department has decided to let the industry regulate itself and issued the following recommendations:

- Web sites should disclose when they are collecting information about users and outline what they will do with the data;
- Visitors should be given the option to determine how the information may be used;
- Medical records should not be shared without a patient's consent; and
- Companies should be held accountable when privacy policies are violated.

A report this year by the California HealthCare Foundation revealed that most health-related Web sites were not honoring their promises to keep personal information about visitors private. The study concluded that all but 3 of 19 Web sites surveyed were violating their own privacy policies. The results are being held up by privacy advocates of their longtime contentions that self-regulation of the Internet is ineffective.[27]

Data Dealing – A Lucrative Business

In the late 1970s a profession known as information brokering came into existence. Information brokers were generally former librarians or researchers who used their computer and research skills to assist attorneys and physicians in locating information for litigation and medical treatment. The early information brokers often searched specialized legal and medical databases to obtain information. In addition, some of the research was done manually. Recent advances in computer technology during the 1990s changed the landscape of information brokering.

The information for sale today is more personal in nature and can be acquired quickly and inexpensively from the thousands of "data dealers" or "data sellers" doing business over the Internet. With numerous recent arrests of data sellers, the image of information brokering has a severely tarnished reputation. These data dealers acquire as much personal data as possible including: marketing lists, bankruptcy records, tax liens, civil judgements, criminal histories, deaths, real estate ownership/transfers, driving records, voter registration, professional licenses, telephone directories, consumer credit reports, financial services records, college directories, and business customer lists. The data is then merged together to create personal "profiles" on individuals and sold to anyone who is interested. These companies generally post legal disclaimers stating they are not liable for the accuracy of the data they sell.

Acxiom, a large data warehouse, sorts people by income, age, race, ethnicity, and geography. Companies like 1-800U.S.Search, American DataLink, A1-Trace USA, Discreet Data Systems, and Dig Dirt boast their services on web sites, claiming to provide anyone's Social Security number, current and past address, unlisted telephone number, date of birth, and alias.[28] Some companies will provide you with someone's financial data as well. Lexis-Nexis, the computer-assisted legal research database provider used by legislatures, lawyers, and law students, recently expanded its services to include an online personal tracking system that provides personal information about millions of people. The Lexis-Nexis P-Track Personal Locator File provides addresses, former addresses, and maiden names among its information. Lexis was including Social Security numbers as well, but decided to remove them.[29] (For examples of the types of information sold by data dealers over the Internet, refer to Attachment C.)

R.L. Polk & Co. is the oldest US consumer marketing information provider, offering demographic and lifestyle information on more than 100 million US and Canadian households. Last year, R.L. Polk was the highest bidder of New York State's vehicle registration lists. Its annual National Vehicle Population Profile provides the auto industry with statistics on about 200 million vehicles in the US and Canada. In response to automotive dealers' requests for a comprehensive, in-house marketing tool, the Polk Company recently introduced its "Polk Dealer Marketing Manager." It is a database system that collects customer data electronically from the

dealers' management system, cleanses those records for accuracy, and combines them with Polk's consumer information to create a customer contact list for dealers. Recently, Polk reached an agreement with HotData Inc. (the leading provider of customer information) to deliver consumer "psychographics and demographics" directly into desktop software applications via the Internet. Marketers from small business will now have greater access to profile customers.

INTERNET TERMS[30]

BBS (Bulletin Board System) – A BBS is a local computer that can be called directly with a modem. Usually they are privately operated, and offer various services depending on the owner and the users. Often a BBS is not connected to a network of other computers, but increasingly BBSs are offering Internet access.

Browser - Software that enables you to navigate the Internet and visit web sites. The major browsers are Netscape Navigator and Microsoft Internet Explorer.

Commercial Online Service - A service in which users pay a certain fee to dial into what is essentially a very large BBS. These services provide a wide range of conferences, forums, software files, news and information, as well as e-mail service. Examples include Prodigy, Compuserve, America Online, the Microsoft Network, and others. Many of these services offer access to the Internet.

Cookies - A feature of many web browsers defined as client-side persistent information. Cookies allow web sites to store information about your visit to that site on your hard drive. Then when you return, cookies will read your hard drive to find out if you have been there before. The web site might offer you products or ads tailored to your interests, based on the contents of the cookies data.

Cyberspace - The "place" where online activities occur. Commentators have noted that many of the activities that take place online are analogous to activities that occur in physical space. These online activities are said to take place in cyberspace.

FTP - Stands for File Transfer Protocol, a system of file storage on the Internet that allows users to upload or download entire files.

Internet - An immense global network of computers. The Internet is not owned by any one entity, but rather owners of individual computer systems agree to participate in it. Users with an account with one of these computers generally may connect with any other computer on the network.

ISP - Stands for Internet Service Provider, a service that provides subscribers with direct access to the Internet. Some of the larger ISPs include Netcom, Pipeline, and Earthlink. Many small, local ISPs exist.

Junk e-mail - Unsolicited commercial electronic mail, also known as "spam."

Modem - Acronym for modulator/demodulator. Equipment which converts the digital signals of your computer (the 1s and 0s) into analog signals which can be transmitted over the telephone network, and vice-versa.

Newsgroups - Newsgroups are lists of messages from users grouped by specific topics. Usenet is a network of thousands of these electronic conferences which may be accessed on the Internet. Most commercial services and BBSs have similar public forums.

Online - Connected to a computer network.

Search engine - A function that enables you to search for information and web sites, often using key words. Some of the commonly used search engines are Yahoo, Lycos, and Excite.

URL - Stands for Uniform Resource Locator. URLs are unique addresses assigned to every location on the Internet. URLs for web pages begin with the letters "http://" usually followed by "www" and the remainder of the address.

Web site - A location on the World Wide Web which can be visited by Internet users employing software called a browser. Every web page is identified by a unique address, called a URL.

WWW - Stands for World Wide Web. This powerful tool for accessing the Internet combines graphics, "point and click" navigation commands, and a method of linking many different sites to allow users to quickly and easily search for information on the Internet.

FINANCIAL SERVICES

In the last decade, the financial services industry has become a colossal information industry that compiles and uses large amounts of personal information. Information generated from personal records (e.g., transaction and check history, credit lines, savings account information, mortgage data) is sold to or shared by banks with affiliates (subsidiaries) as well as third parties, who in many cases, collect and compile this personal information to be sold to direct marketers and "data dealers." Historically, the financial services industry has been regulated to protect the finances of the public. But with respect to the treatment of personal information, federal and state statutory protections have been very limited, focusing primarily on government's use of personal financial data.[31]

For approximately 60 years, banks were prohibited from merging with insurance companies. However, due to the recent enactment of the federal Financial Services Modernization Act (P.L. 106–102), it can be expected that a number of banks will take advantage of the ability to now merge with other entities creating "one-stop-shopping" businesses. This in turn may open the flow of personal information at an unprecedented rate. The federal bill contained an opt-out provision for consumers that do not want their information shared with third parties but did not give individuals the right to opt-out of having their information shared with bank affiliates, which could include any type of private entities including: insurance companies, securities firms, airlines and retailers. The legislation allows states to enact stricter measures.

Unlike European regulations, the U.S. generally does not place restrictions on the secondary use of personal information by financial institutions such as payment information and credit card transactions.[32] A few states have laws that prohibit financial institutions from disclosing customer records to third parties without the customer's consent.[33] Chase Manhattan Corp. recently agreed to end its practice of supplying outside marketers with customers' personal and financial information without consent. The Task Force supports the move by Chase Manhattan and other financial institutions to receive customer consent prior to the release of personal information.

Task Force Bank Survey

Privacy policies vary considerably across the financial services industry with some institutions, such as Citigroup, articulating detailed policies with opt-out provisions and others having none. At present, financial institutions are recognizing the public concern regarding personal information and many are beginning to address the issue. In order to better ascertain the extent to which financial institutions use customer information for purposes not related to customer account maintenance or transaction purposes, the Task Force surveyed a random sample of 50 banks in New York State regarding their collection and use of customer information. Thirty-two institutions (64%) responded to the survey; the results are summarized below:

- Institutions were asked if they used customer (account holder) information to market bank-related products and services as well as to market unrelated products and services:
  59% of respondents said they used information for bank-related purposes only
  41% said the information was used for purposes not directly related to banking

- When asked if customer information was shared with other financial institutions, affiliates (subsidiaries) as well as nonaffiliates:
  71% of respondents said they shared information with other institutions – most said they shared pre-selected lists with credit card and investment companies.
  29% of respondents said they did not share the information with any other parties.

- Institutions were asked if they shared customer information with nonfinancial institutions (e.g., insurance companies, marketers):
  53% of respondents said they did not share customer information and 47% said they did

- Institutions were asked if they had a detailed privacy policy for customer information:
  58% of respondents said they did not have such a policy
  41% of respondents said they did have such a policy (of the 41%, 30% had policies relating only to Internet banking services)

- Institutions were asked if they provided any notice to customers that information about them would be disseminated to other entities or used for marketing purposes:
  60% of respondents said no notice was provided to customers
  28% of respondents said they did at some time (usually when opening an account) notify customers
  12% N/A

- Institutions were asked if they allowed customers to refuse the disclosure of personal information to other parties:
  53% said they allowed customers to opt-out by request
  29% said they did not allow customers to opt-out
  18% N/A

CREDIT REPORTING AGENCIES

Among the largest information databases are those controlled by the nation's 3 credit bureaus – Equifax, Trans Union, and Experian (formerly TRW). These entities reportedly hold records on 160 million individuals. Individual credit files generally include birth dates, family make-up, current and previous addresses, telephone numbers, Social Security numbers, employment and salary histories, credit transactions and balances, bankruptcies, tax liens and legal information. The credit bureaus serve as information clearinghouses, receiving charge and payment transaction information from businesses that grant consumer credit and providing businesses with consumer credit reports.[34] This vast array of information is often sold to credit grantors, landlords, employers, insurance companies, and other parties, without individuals' knowledge or consent.

The federal Fair Credit Reporting Act (FCRA) places some restrictions on credit agencies' ability to share or sell information in people's credit reports. Only those specified as having a "permissible" business purpose are allowed access to this information. Those allowed access usually are limited to an application with a creditor, insurer, employer or landlord. However, the large credit holding companies are allowed to share credit reports and credit applications among their affiliates that do not have a permissible purpose to look at a citizen's report. The credit bureaus get around the "permissible" business provision by selling what is referred to as "header information." This information may include a person's Social Security number, income, age, unlisted telephone number, and address (but not the complete consumer credit report). Once creditors, insurers, or any other entity obtains information about a person, they may use it as a basis for sending out unsolicited offers.

In 1998, Trans Union was ordered by the Federal Trade Commission (FTC) to stop selling personal financial information to catalogers, telemarketers and other target-marketing companies. Administrative Law Judge James Timony, wrote in a decision that Trans Union "invades consumers' privacy when it sells consumers' credit histories to third-party marketers without consumers' knowledge or consent."[35] According to the FTC, Trans Union's clients for its target-marketing business have varied widely, including: an auto insurer, banks, catalogers, and Publisher's Clearinghouse.[36] Trans Union is appealing the decision, claiming that it has the right to share the information since it is not "consumer report" information.

Equifax recently announced it is acquiring the consumer division of R.L. Polk & Co. for about $260 million. This purchase would give the credit company a greater presence in the business of compiling and sorting personal information, including lifestyle preferences for marketing purposes. In addition to the vast amount of personal information Equifax holds, it will soon obtain consumer data about 105 million households.[37]

It has been suggested that some of the practices of credit reporting agencies may have contributed to the increase in identity theft. Pre-approved credit offers, the sale and distributions of "header information" and a lack of verification by credit grantors have been blamed. Because of this, and the roughly 30% error rate on credit reports, a number of lawmakers have supported legislation to provide free annual credit reports. Massachusetts, Vermont, New Jersey and Maryland, are among the states that have enacted such legislation.

To contact the 3 credit bureaus, use the information provided below

Equifax — www.equifax.com
To order your report, call: 800-685-1111 or write:
P.O. Box 740241, Atlanta, GA 30374-0241
To report fraud, call: 800-525-6285 and write:
P.O. Box 740241, Atlanta, GA 30374-0241

Experian — www.experian.com
To order your report, call: 888-EXPERIAN (397-3742) or write:
P.O. Box 949, Allen TX 75013-0949
To report fraud, call: 888-EXPERIAN (397-3742) and write:
P.O. Box 949, Allen TX 75013- 0949

Trans Union — www.tuc.com
To order your report, call: 800-916-8800 or write:
760 Sproul Road, P.O. Box 390, Springfield, PA 19064-0390
To report fraud, call: 800-680-7289 and write:
Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634

INSURANCE COMPANIES

Insurance companies collect and retain a considerable amount of personal information. With the recent enactment of the federal Financial Services Modernization Act, it can be expected that a number of insurance companies may become affiliated with banks. When such partnerships are formed, one entity has access to and can share an individual's financial as well as health/medical data. Concern has been raised that an instance could conceivably transpire whereby an individual would be denied borrowing privileges by his or her bank after the discovery that he or she has a terminal illness. While such an occurrence may be rare, it is nonetheless possible. The recent federal legislation does not allow individuals to opt-out of affiliate sharing – state legislation would be required to do so. A number of states including California, Illinois, Massachusetts and Maryland place restrictions on the disclosure of personal information held by insurers.

OTHER BUSINESSES

Some retail and food merchants keep considerable customer information in their databases such as names, addresses, phone numbers, Social Security numbers, credit card numbers and purchase information. These businesses often provide a "reward" in the form of a "frequent shopper card" or coupons to their customers for sharing their personal information. The information is used by merchants for their own marketing purposes and is sometimes shared or sold to third parties. Arguably, there are some benefits associated with retailers and merchants maintaining customer information, particularly, the ability to tailor services to customers' preferences. However, advances in technology raises concern about the type of information that merchants and retailers are able to retain. For example, with sophisticated data readers, when a drivers' license is swiped, picture, height, weight, and eye color could be captured allowing businesses to build their own private FBI databases. Should this information find its way into the database of an unethical third party, the unsuspecting consumer could be victimized.

TELEMARKETING

"The right to be left alone -- the most comprehensive of rights, and the right most valued by a free people."

Justice Louis Brandeis (1928).

In 1996, Attorney General Dennis Vacco announced the results of a statewide telemarketing survey that found that one in five New York State residents polled had fallen prey to unscrupulous telemarketers. It is estimated that 10% of the 140,000 telemarketers across the country represent fraudulent businesses. An individual may reduce the number of telephone solicitation calls to his/her home by contacting the Telephone Preference Service of the Direct Marketing Association (DMA). The DMA publishes a list of consumers who do not wish to receive future telephone solicitations. However, these "do-not-call" lists must only be followed by member organizations of the DMA which constitute a small number of all telemarketing companies.

Recently, a number of states have enacted legislation establishing state "do-not-call" lists that telemarketers must adhere to. Florida State Law (Section 501) prohibits sales solicitation calls to consumers who have placed their names on Florida's "no calls" list. There are exceptions however, such as: if the call is regarding an existing debt or contract or if the telephone solicitor has a prior or existing business relationship with the person being contacted. Florida's "no calls" statute allows any residential, mobile, or telephonic paging device telephone subscriber to place his or her name on a "no sales solicitation calls" list for a $10 initial fee, with an annual renewal cost of $5. According to state officials, a considerable amount of revenue has been raised with the imposition of fines against telemarketers that have not abided by the law.

PRIVACY AND CHILDREN

Evolving online networks offer golden opportunities for advertisers and marketers. They are using these networks to gain direct access to children of all ages from preschoolers to teens. The sooner they can turn them into obliging consumers, the better. In the past decade, children have become an extremely valuable market. In 1995, children under twelve spent $14 billion, teenagers another $67 billion, and together they influenced $160 billion of their parents' annual spending. In addition to having unprecedented spending power, children are early adopters of high-tech products, making them a disproportionately important market for the new interactive media.[38] Competition for consumers coupled with an increase in Internet use could put society's most vulnerable citizens in danger. Here are a couple of examples:

Look-up services allow strangers to locate children
"There is no law on the books that prevents a stranger from calling a 900-number and getting information about your children. In fact, until a few weeks ago, a subsidiary of R. Donnelley provided a service that did just that."
CNN, December 14, 1995.

Kids' data disclosed to investigative reporter posing as child murderer
"To prove how easy it is for pedophiles to obtain mailing list of kids, a Los Angeles television station reported that it obtained a detailed computer printout of the ages and addresses of 5,500 children living in Pasadena simply by sending $277 to a Chicago database firm."
The San Francisco Examiner, May 12, 1996.

THE CHILDREN'S ONLINE PRIVACY PROTECTION ACT

In response to concern over the safety of children using the Internet, the Children's Online Privacy Protection Act was recently enacted and becomes effective April 21, 2000. The regulations apply to the online collection of personal information from children under 13. They specify what a Web site operator must include in a privacy policy, when and how to seek verifiable consent from a parent and what responsibilities an operator has to protect children's privacy and safety online. The regulations apply to commercial Web sites or online services directed to children under 13 that collect personal information from children. To determine whether a Web site is directed to children, the FTC will consider several factors, including the subject matter; visual or audio content; the age of models on the site; language; whether advertising on the Web site is directed to children; information regarding the age of the actual or intended audience; and whether a site uses animated characters or other child-oriented features.[39]

The Children's Online Privacy Protection Act and Rule apply to individually identifiable information about a child that is collected online, such as full name, home address, email address, telephone number or any other information that would allow someone to identify or contact the child. The Act and Rule also cover other types of information - for example, hobbies, interests and information collected through "cookies" or other types of tracking mechanisms - when they are tied to individually identifiable information.[40]

The regulations also requires operators to post a link to a notice of its information practices on the home page of its Web site or online service and at each area where it collects personal information from children. A notice to parents must contain the same information included on the notice on the Web site. In addition, an operator must notify a parent that it wishes to collect personal information from the child; that the parent's consent is required for the collection, use and disclosure of the information; and how the parent can provide consent. An operator must give a parent the option to agree to the collection and use of the child's personal information without agreeing to the disclosure of the information to third parties. That is, a parent can grant consent to allow his/her child to participate in activities on the site without consenting to the disclosure of the child's information to third parties.[41]

At any time, a parent may revoke his/her consent, refuse to allow an operator to further use or collect their child's personal information and direct the operator to delete the information. The regulations include several exceptions that allow operators to collect a child's e-mail address without getting the parent's consent in advance. These exceptions cover many popular online activities for kids, including contests, online newsletters, homework help and electronic postcards.[42]

STUDENT RECORDS

Under the federal Family Educational Rights and Privacy Act (FERPA) (20 USC Section 1232g), students' school health records, report cards and disciplinary files are categorized as "privileged documents," generally not to be disclosed except as required by law. FERPA requires that student records be disclosed to parents or eligible students. Disclosure to anyone else is limited. A common practice of schools is the printing of student "directory information." FERPA requires educational agencies to give notice of the type of information they will include in their directories and allow a reasonable period of time after such notice is provided for parents to inform the educational institution that any or all the information should not be released.

Higher education institutions use SSns for a broad range of purposes some of which are required by State and federal law, such as for financial aid or employment. However, a number of colleges post students' SSns on student identification cards and on class lists. In some cases, the numbers may be accessed over the Internet and some faculty use them to post student grades. In recent years, some institutions have recognized the need to safeguard students' SSns and have implemented internal controls to limit use of them.

Student directories are sought by marketers, some who post the information on the Web. Also, credit card companies buy student information in order to target students for credit cards. Unfortunately, there have been cases where stalkers have used the information in directories to stalk female students. Students should be aware that educational institutions may sell the personal information in the directories. Pedophiles sometimes try to acquire lists of names of students in nearby schools. When doing so, some have been known to post the information on the Web.

MEDICAL INFORMATION

"What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself holding such things shameful to be spoken about."[43]

Hippocratic Oath: Fifth Century B.C.

As sensitive as financial information is, medical records are even more so. Personal health care records can include an individual's medical, psychiatric, or psychological history, diagnosis, condition, treatment, evaluation, or drug prescriptions. The single most difficult issue fueling the debate about access to medical records is how to protect an individual's privacy while allowing justified research and billing access to personal health data. Patients are growing increasingly uneasy about the easy accessibility of their health care information. In response, in 1998, at least 35 state legislatures introduced bills clarifying the boundaries between confidentiality and privacy of medical records and rightful access to computerized health information by qualified medical researchers, insurers and employers.

At first glance, medical records appear to be one of the areas where our personal information is kept private. Most states have laws that require doctor-patient confidentiality. But these laws generally contain exemptions in most cases for insurance coverage.[44] When patients sign waivers or consent forms, their medical records may be released to insurance companies, government agencies and others. The proliferation of managed care organizations has, in effect, created tremendous storehouses of medical records information. Medical information gathered by one insurance company may be shared by others through the Medical Information Bureau (MIB). The MIB is the largest repository of medical records in the United States and Canada. According to *PC World*, this consortium of insurance companies maintains millions of records culled from insurance applications as well as from doctors' and hospitals' files. When someone applies for insurance, insurers scan MIB's computers for information about any preexisting conditions that might affect their decision to issue the policy or how much to charge.

On occasion, MIB files end up in the wrong hands. There are cases of employers using the information to discriminate against prospective employees and marketers using them to target consumers. For example, Elensys, a Massachusetts company, manages customer records for pharmacies and uses the files for marketing purposes, often on behalf of drug manufacturers. According to George Lundberg, M.D., editor in chief of the *Journal of the American Medical Association*, this practice is "a gross invasion" of privacy.[45] In addition, journalists often access medical records for a number of reasons, including: reports on traffic accidents, disasters, and the health of public officials.[46]

A Massachusetts judge recently denied a motion by a pharmacy chain and several pharmaceutical companies to dismiss a suit by two men who claim their privacy rights were violated by a joint marketing plan under which the pharmaceutical firms used pharmacy records to send mailings to customers containing disease-specific marketing materials (*Weld et al v. CVS Pharmacy Inc.*, No. 98-0897F).[47] The program, since discontinued by CVS, and funded by pharmaceutical companies provided for release to mailing houses (on behalf of the drug

manufacturers) of names and addresses of CVS customers that had specific illnesses. These customers were then solicited by drug companies to consider their products. Apparently, CVS shared personal information in other states as well. Discovery of this practice in South Carolina prompted the passage of R. 154, Laws of 1999, enacting the Prescription Information Pharmacy Act. The law prohibits patient prescription drug information from being transferred without the written consent of the patient.

A Consumer's Complaint Regarding Rite Aid Pharmacy

August 1999

Note: The following letter was written by a customer of the Rite Aid Pharmacy about its marketing practices. It was shared with the Privacy Rights Clearinghouse and permission was granted to post it. Rite Aid has recently been the subject of several media reports about its aggressive marketing of pharmaceutical products and other consumer-unfriendly practices, including selling date-sensitive products well past the due dates. Rite-Aid is the largest pharmacy chain in California. It has recently been investigated by government regulators in California, Washington, and Oregon.

California Department of Consumer Affairs
Board of Pharmacy
400 R Street., Ste 4070
Sacramento, CA 95814

To Whom it May Concern:

I am writing to complain about Rite Aid Pharmacy. Recently, Rite Aid sent me a letter, sponsored by a pharmaceutical manufacturer, to "remind" me to refill a particular prescription medication that I am taking. Shortly thereafter, someone at our local Rite Aid called my husband to "remind" him to refill a particular prescription medication that he is taking. They told my husband that they could have his prescription ready and waiting for him.

I feel that Rite Aid is using my family's private medical information -- our prescription records -- to aggressively market prescription medications on behalf of themselves and pharmaceutical manufacturers. I find this to be an egregious invasion of my privacy and am concerned that Rite Aid may be violating laws in California regarding my medical records privacy. At the very least, I consider this to be unprofessional conduct.

Rite Aid should be filling prescriptions upon the request of an individual and his or her physician, not upon the request of the pharmaceutical manufacturer.

Thank you for your time and attention to this matter.

Sincerely,
Lisa G

Medical information may be passed on to direct marketers when you participate in informal health screenings. Results from tests for blood pressure, cholesterol levels, and physical fitness often conducted at fairs, pharmacies and shopping malls, find their way to businesses interested in marketing health-related products.[48] Another way that personal medical information may become shared is through the Internet. Many Usenet news groups and chat rooms exist for individuals to share information with others who have similar conditions and diseases. There is an abundance of anecdotal evidence that such information has been collected and distributed without consent.

For several years, Congress has debated the issue of imposing a health identifier number on all Americans in order to build a national database of health information. Proponents contend that such a move would allow doctors expedient access to a patient's medical history during life-saving procedures. However, privacy advocates opposed creation of a national database of personal medical history, claiming it would destroy doctor/patient confidentiality. Under a law passed in 1996, the Congress was to enact medical privacy protections by August of 1999. Since Congress did not act by the deadline, the Secretary of the U.S. Department of Health and Human Services has been given the authority to promulgate regulations**.** The regulations placed some restrictions on individually identifiable health information while giving patients access to their records. Some privacy advocates claim the regulations do not adequately personal medical and are urging Congress to enact legislation to do so.

Sections 17 and 18 of the Public Health Law concern the release of medical records, access to patient records, and disclosure to third parties. In addition to the patient, the following parties have access to patient records: medical access review committees, health care providers, health care practitioners, and health care facilities. The New York State Department of Health is a significant repository of health related data. Individual identifying data is not generally released in response to a FOIL request. This data is withheld pursuant to the FOIL provision allowing agencies to withhold information, which, if released, would constitute an unwarranted invasion of personal property.

FEDERAL PRIVACY LAWS

There is no comprehensive law that addresses the use of personal consumer information across all industries. Rather, a patchwork of state and federal laws deals with issues of personal privacy in the commercial context. They include:

Cable Communications Policy Act of 1984 (47 USC §521 et seq., §611)—This act addresses concerns about the ability of interactive cable systems to track cable consumer viewing or buying habits. It prohibits the collection of personally identifiable information without the consumer's prior consent except as needed to render service provided by the operator or to prevent interception.

Children's Online Privacy Protection Act of 1998 (15 USC §§6501-6506)—This act prohibits the collection of information about children under the age of 13. The law gives rule-making authority to the FTC to address issues like parental notification and consent prior to the collection of information from children. The FTC enacted such rules in 1999. The law also recognizes a "safe harbor" option that would allow industry members to submit self-regulatory mechanisms to the FTC and be deemed in compliance with the law.

Communications Assistance for Law Enforcement Act of 1994 (47 USC §§1001-1-10; §1021; 18 USC §2522)—This act establishes protection for cordless telephone conversations and establishes a warrant requirement for government access to e-mail addresses.

Driver Privacy Protection Act of 1994, and as amended in 1999 (18 USC §§2721-2725)—This law protects state motor vehicle records and restricts their dissemination to only authorized parties and in many instances only for specified purposes. The 1999 amendments tie state compliance to the appropriation of federal transportation funds for states.

Electronic Communications Privacy Act of 1986 (18 USC §1367, § 2232, §2510 et seq., §2701 et seq., §3117, §3121 et seq.)—This act protects all forms of electronic transmissions, including video, text, audio and data from unauthorized interception.

Electronic Fund Transfer Act (15 USC § 1693)—The law requires financial institutions to include in an initial account disclosure the circumstances under which it will disclose information to third parties.

Fair Credit Reporting Act (15 USC §1681 et seq.)—This law regulates the disclosure of personal information by consumer credit reporting services. It requires such services to adopt reasonable procedures to ensure the accuracy of personal information contained in their credit reports. It also offers a process for consumers to review and correct inaccurate information on a credit report. Credit report information can be shared with affiliates when a consumer is told the information may be shared and is given the opportunity to opt out from information sharing with affiliates. It does not restrict the amount or type of information to be released to third party inquirers when the reporting agency has reason to believe it will be used for credit, employment or insurance evaluations or other "legitimate business needs" affecting the individual consumer. The law is silent about sharing transactional, experiential information. This silence has been

interpreted by the Office of the Comptroller to mean that the information can be shared freely with third parties.

Federal Credit Union Act (12 USC § 1751 et seq.)—This act mandates the promulgation of standard bylaws that all federally chartered credit unions must adopt. These bylaws require that all personal information be held confidential except to the extent necessary to make loans, extend credit, collect loans and guarantee share drafts.

Family Education Rights and Privacy Act of 1974 (Buckley Amendment) (20 USC §1232g)—This act protects the accuracy and confidentiality of student records.

Federal Trade Commission Act (15 USC §41 et seq.)—This act, which creates the Federal Trade Commission ("FTC"), establishes among other things consumer fair business practices and gives the FTC jurisdiction and authority to address unfair, deceptive or misleading business practices.

Federal Privacy Act (5 USC §552a)—This act establishes a code of fair information practices applicable to government record-keeping and empowers individuals to discover, correct and control dissemination of sensitive personal information in the government's possession. This act also limits circulation of identifiable personal information and prohibits government from selling or renting an individual's name and address unless specifically authorized to do so by law.

Financial Services Modernization Act of 1999 (Pub L. 106 – 102, November 12, 1999)--The main thrust of this law is to allow financial institutions to merge with insurers and securities firms so that they can consolidate services. It does not preempt states from regulation. The act requires financial institutions to adopt written privacy policies and to disclose those policies to consumers. It gives the consumer a right to opt out of most disclosures of personal information to third parties, but does not address affiliate sharing of personal information. It prohibits third parties from redisclosing personal financial information. It provides detailed requirements for notice and creates rule-making authority for federal agencies. It prohibits disclosure of certain highly sensitive account and password information to third parties for use in marketing. It also increased penalties for identity theft.

Identity Theft and Assumption Deterrence Act of 1998 (Pub L. 105-318, Oct. 30, 1998, 112 Stat. 3007)—This law enacts no new sections of law but amends existing laws. It criminalizes fraud in connection with unlawful theft and misuse of personal identifying information itself, regardless of whether it appears or is used in documents. Previously, only the fraudulent creation, use, or transfer of identification documents was illegal, not theft and misuse of personal identifying information itself. The criminal provisions are enforced by the U.S. Department of Justice. The law requires the FTC to create a centralized complaint and consumer education service that will log complaints, provide informational materials and refer complaints to the appropriate entities, including consumer reporting and law enforcement agencies.

Privacy Protection Act of 1980 (42 USC §2000aa et seq.)—This act guards against law enforcement searches and seizures, without a warrant, of materials intended for publication, extending, as some commentators believe, to materials intended for publication on online systems or bulletin boards.

Right to Financial Privacy Act of 1978 (12 USC §3401 et seq.)—This act protects against disclosure to government of personal financial records held by banks, except with a search warrant.

Telephone Consumer Protection Act of 1991 (47 USC §227, §331)—This law provided the basis for the FCC rule requiring persons engaged in telemarketing to maintain a list of consumers who request not to be called. It also prohibits junk faxes and automatic dialing and announcing devices.

Video Privacy Protection Act of 1988 ("Bork Bill") (18 USC §2710, §2711)—This act prohibits disclosure of video customer rental records. Customer names and addresses can be disclosed for direct marketing purposes unless the customer prohibits this use.

Source: Consumer Privacy Workgroup Report To The Attorney General Of The State Of Washington. January 10, 2000.

SOME 1999 FEDERAL PROPOSALS AIMED AT PROTECTING PERSONAL INFORMATION

- Prohibits the use of Social Security numbers except for Social Security or Internal Revenue Service purposes (HR 220);

- Forbids the commercial use of compiled data by a third party without permission (HR 354);

- Prohibits financial institutions and their employees from disclosing a customer's financial records, but would not supersede state laws (HR 30);

- Prevents Internet service providers from disclosing personal information about their customers without written permission (HR 313); and

- Makes it a federal crime to stalk a person, enter onto private property to tape or record them, then attempt to sell the recording to someone (HR 97).

- The "Personal Information Privacy Act of 1999" amends the Fair Credit Reporting Act in relation to "header information" released by credit agencies; prohibits from providing a consumer report unless the consumer initiates the transaction or provides consent; prohibits the commercial acquisition or distribution of an individual's Social Security number without consent; and prohibits the use of one's Social Security number as a personal identifier (H.R.1450).

- The Social Security On-line Privacy Protection Act prohibits "interactive computer services" from disclosing Social Security numbers or using the social security number as an identifier to disclose personal information (HR 1287)

RECENTLY INTRODUCED (1999 & 2000) PRIVACY LEGISLATION IN THE NEW YORK STATE SENATE*

EZ-PASS/ELECTRONIC TOLL RECORDS PRIVACY

S. 4413 (TRUNZO) - Amends the Public Authorities Law to protect the confidentiality of electronic toll collection system (EZ-Pass, Metrocard) customer account information. Provides exemptions for law enforcement purposes, disclosure pursuant to court order and account administration. (See also S.850 (BALBONI), S.816 (HANNON)).

PUBLIC RECORDS AND EMPLOYEES' PRIVACY

S.3592 (LACK) - Amends the Civil Rights Law to protect the privacy of county clerks with respect to their personnel records. It would afford county clerks the same privacy rights given to other court officers, bridge and tunnel officers, sergeants and lieutenants.

S.4276 (VOLKER) - Amends the Civil Rights Law to protect the privacy of parole officers with respect to their personnel records. Similar to S.3592, but would expand statutory confidentiality to "peace officers" records.

S.3231 (DEFRANSISCO) - Amends the Civil Rights Law to limit the disclosure of public records containing personal information when they are sought for purposes unrelated to the purpose for which they exist.

S.1962 (JOHNSON) - Amends the Penal Code to create a new category of crime (Class E felony) for the use of government documents for the purpose of advancing criminal activity.

CREDIT REPORTING & FINANCIAL INFORMATION

S.1586 (NOZZOLIO)- Amends the General Business Law to require written consent prior to a credit reporting agency or creditor furnishing information to a third party. Provides for consumer notification and opportunity to have their name removed from the mailing list. (See also S.530 (NOZZOLIO)).

S.1597 (LACK) - Enhances the consumer credit reporting protections for New York State residents. Creates statutory requirements for verification of identity and an advertised toll free number for consumers to communicate with credit reporting agencies. This bill is modeled after federal law.

S.4452 (DEFRANSISCO) - Requires issuers of credit cards, charge cards, or debit cards who sell, rent, or exchange customer information to inform the customer of this practice on at least an annual basis and requires the issuer to instruct the customer on how they may prevent the exchange of this information.

S.3461 (VELELLA) - Requires credit card issuers to implement as a fraud prevention measure telephone confirmation including proof of identity, prior to activation of offers of credit. Prohibits applications offering pre-approved credit cards from indicating their contents on the envelope. (See also S.3914 (VELELLA)).

S.2190 (MALTESE) - Amends the Penal Law to make it illegal to possess stolen credit card or similar numbers (i,e., .PINS) and criminalizes the possession of stolen electronic or written codes of a cellular phone.

TELEMARKETING

S.5947 (MAZIARZ) - Amends the General Business Law to require telemarketers to be registered and bonded with the Department of State. Establishes code of conduct and creates civil fines and penalties. Prohibits use of courier pick-up for prepayment of goods and requires consent and verifiable authorization for access to bank, saving or similar account information over the phone.

S.512 (SEWARD) -Requires each local exchange telephone company to arrange for the establishment and administration of a registry listing the telephone numbers of residential telephone customers who wish to avoid the receipt of telephone solicitation calls and the name and address of each New York telemarketer. (See also S.5410 (GOODMAN)).

CRIMINAL ACTIVITY/ VICTIMS'

S.1188 (GOODMAN) - Amends the Penal Law and General Business Law to prohibit identity theft. "Identity theft" is defined as: knowingly obtaining any personal identifying information of another person with the intent to use that information to obtain, or attempt to obtain credit goods, money or services in the name of the other person or to cause financial loss to the other person without their consent.

S. 4062 (NOZZOLIO) – Amends the Penal Law, Creating the crime of "cyberstalking".

S.853 (BALBONI) - Amends the Civil Rights Law to provide that a victim or witness to a crime need not be required to disclose his or her home address or telephone number in open court. (See also S.4278 (VOLKER).

S.1741 (JOHNSON) - Amends the Civil Rights Law to prohibit disclosure of felony crime scene photographs, except where disclosure is to public officers and employees for an investigation, prosecution, record-keeping purposes or for purposes of a criminal or civil trial.

S.1215 (VELELLA) - Amends the Civil Rights Law to provide for the confidentiality of victims' and witnesses' business and residential addresses and telephone numbers.

S.704 (NOZZOLIO) - Amends the Civil Rights Law to specifically deny prisoners the ability to obtain agency records, except under certain circumstances. Requires inmates seeking information through FOIL to indicate their status as inmates and to state the purpose for which they are seeking such information.

S.3231 (DEFRANSISCO) - Amends the Civil Rights Law to limit disclosure of records with personal information unless the person requesting such information can demonstrate that the request is for a lawful purpose and that such purpose relates to the reason for which the record exists. (Similar to S.704)

S.5200 (MAZIARZ) - Amends the Civil Rights Law to prohibit the publication or broadcasting of information identifying a sexual offense victim.

INTERNET PRIVACY

S.722 (RATH) - Regulates the transmission of unsolicited commercial electronic mail advertising. (See also S.5090, S.5283 (FUSCHILLO).

INSURANCE & HEALTH RECORD PRIVACY

S.2429 (VELELLA) - Creates a new article of the Insurance Law on Information and Privacy Protection. Establishes the regulatory requirements for the collection and dissemination of personal and confidential information that is used in the underwriting for health, life, and disability insurance. (See also S.3860 (SEWARD).

S.1687 (FARLEY) - Prohibits the disclosure of health care information or personal information to a person who engages in the business of accessing information and compiling information for commercial purposes or whose use of such information will be in connection with the marketing of a product or service without the explicit written authorization of the data subject.

MISCELLANEOUS

S.4453 (DEFRANCISCO) - Requires publishers of newspapers, magazines, or other periodically printed material to inform customers on at least an annual basis they may sell, rent, or exchange customer information. Notice must also inform the consumer that he or she has the option of prohibiting the release of this information.

S.4648 (SKELOS) - Amends the General Business Law regulate mailing unsolicited advertisements in order to give consumers the right to opt-out of future mailings.

S.2790 (MARCELLINO) - Amends the Penal Law to prohibit unlawful video surveillance in private place.

S.5074 (SKELOS) - Amends the Civil Rights Law to require anyone who provides good and services and who collects and maintains personal information of customers, shall "destroy" records containing personal information prior to discarding such documents.

S. 6237 (FARLEY) - Prohibits the use by public or private schools and colleges of student Social Security numbers as student identification numbers or for any student identification purposes except the employment of a student by a college.

* These privacy bills have been introduced for consideration in recent years by Senate Majority members. The Task Force expects that additional bills will be introduced during the 2000 legislative session.

RECENTLY INTRODUCED PRIVACY LEGISLATION IN OTHER STATES

In response to a call by the public for greater privacy over personal information, a number of state legislatures have introduced measures to amend current statutes governing the collection and distribution of personal information. A number of these measures are highlighted below:

California – Enacts the Personal Information and Privacy Act of 1999, which would impose restrictions on the collection and disclosure of personal information by governmental, business, or not-for-profits (SB 129);

California – Permits consumers to opt-out from having supermarkets share or sell their personal information (SB 417);

Connecticut – Makes numerous provisions regarding the protection of individual medical records (Bill 337);

Colorado – Increases the penalties for misuse of confidential medical information (Bill 99-1184);

Florida – Requires consent for the disclosure of personal information about individuals from the Department of Motor Vehicles (HB 43);

Florida – Prohibits the sale of personal information obtained from a database without the consent of the person to whom it pertains (Proposal No. 57);

Illinois – Establishes an Advisory Commission on Internet Privacy (HB 2696);

Minnesota – Enacts the Minnesota Consumer Privacy Protection package requiring "opt-in" provisions for the sale of personal information by financial institutions, HMOs/heath care providers, telemarketers, and government (No bill number assigned yet);

South Carolina – Prohibits patient prescription drug information from being transferred without the patient's consent (Signed by Governor 6/9/99, Act No. 85).

Utah – Provides for the protection and confidentiality of motor vehicle accident reports (HB 330);

Utah – Enacts the Genetic Testing Privacy Act to provide greater patient confidentiality with regard to test result disclosure (HB 177);

Utah – Requires a merchant to provide notice to a customer before selling his of her personal information to any third party (HB 70); and

Vermont – Consolidates and strengthens the privacy and confidentiality safeguards for individually identifiable health care information and clarifies the rights and responsibilities of those who handle health information and records (S 54).

WITNESSES THAT TESTIFIED AT THE SENATE TASK FORCE HEARINGS

Thursday, April 15, 1999, Albany

Alexander F. Treadwell, Secretary of State

Richard E. Jackson, Jr., Commissioner, New York State Department of Motor Vehicles

Maryalice O'Brien, AARP Legislative Committee Chair

Robert Gellman, Privacy and Information Policy Consultant, Washington, DC

Robert Smith, Publisher of the Privacy Journal, Author, Providence, R.I.

Gavin Donohue, Executive Deputy Commissioner, New York State Department of Environmental Conservation

Allan Davies, Assistant Vice President, Data Acquisition, Dun & Bradstreet

Charles Bell, Programs Manager, Consumers Union

Henry Greenberg, General Counsel, New York State Department of Health

Robert Houvener, President and CEO, Image Data, LLC

Hugh Jewett, Vice President, Government Affairs, Telecheck

Thursday, May 27, 1999, Mineola

Professor Joel Reidenberg, Fordham Law School

Donald E. Smith, Identity theft victim

Daniel Troutman, Regional Director of Governmental Relations, The Polk Company

Joan Warrington, General Counsel, Citigroup

Daniel Rowe, Vice Chairman, State Bank of Long Island

Larry Lofaro, private Investigator, Owner of Infosource

Patricia Faley, Vice President, Ethics & Consumer Affairs; Roscoe Burton Starek, Senoir Vice President, Catalog Industry, The Direct marketing Association (DMA)

Thursday, November 18, 1999, Rochester

Cynthia Watkins, Victim of identity theft

James Sherin, Vice Chairman & Director of Governmental Relations, Retail Council of New York State

Russ Davis, Director of Credit Legislative Affairs, Sears

John Gleason, Vice President of Credit, The Bon Ton Stores

Michael Rosen, Vice President & General Counsel, The Food Industry Alliance

Jo Natale, Consumer Services Manager, Wegman's Food Markets

Thomas Gosdeck, Hill & Gosdeck, Albany

Bob Ryan, Trans Union

Bill Brown, Credit Bureau of Rochester

Trudi Bushy, Experian

Emily Hackett, State policy Director, Internet Alliance

Online Privacy Alliance. (Written Testimony Submitted Only)

PRIVACY TIPS BY THE PRIVACY JOURNAL

- Be discreet when filling out application forms - whether on-line or elsewhere. Insert N/A, for "Not Applicable" or "Not Available," or whatever you want it to mean. Phrase your demand so that it elicits a POSITIVE RESPONSE, not a negative one. Don't say, "I refuse. . . ." Say, "Because I'm concerned about my privacy, I chose to keep that information to myself. . . ." Assume that most clerks, as individuals, will identify with your concerns, and you will discover that many of them do. Be persistent. Be prepared to try three or four times before the organization caves in.

- Protect the confidentiality of your Social Security number. (It is the means for a stranger to impersonate you or for a stranger to link information about you from different data bases.) Don't provide it unless the transaction has tax consequences. Never give it out over the telephone or on-line. Always ask why it is needed. Try giving only the last four digits, if you have to. Keep it off your driver's license.

- Ask to inspect and to correct files about yourself. You have a right by law to do this in credit records, federal agency records, school records, criminal records, and (in 20 states) medical records. Even where the law does not recognize your right, assert it anyway. Many companies have promised publicly that they provide this right.

- Subscribe to Privacy Journal to stay current and know your rights. You can subscribe for a special discounted rate of $35 a year when you mention "Privacy Tips" and pay in advance.

- Attach conditions to sensitive information. Ask in writing that it not be disclosed or that it be erased after a certain number of years. This creates a contract with the organization.

- Never provide personal information over the telephone to anyone unless you placed the call and know the organization.

- Ask the post office not to disclose your change of address to commercial mailers. Better still, make your change of address TEMPORARY not permanent. A temporary forwarding instruction is good for one year, and the Postal Service does not forward TEMPORARY change of address information to commercial list users and direct marketers.

- List your telephone number but not your address in the telephone book. This will foil compilers of many marketing lists. Call 800/567-8688 and ask the three major credit bureaus - Equifax, Experian, and Trans Union - that information in your credit report not be disclosed for compiling marketing lists. Call Experian (Metromail) at 800/407-1088 in Lombard, Ill., and Axciom at 501/336-2722 in Conway, Ark., and ask them to remove your name and address from their marketing lists.

- Remember that cellular, mobile, and cordless telephones are not secure and that e-mail is comparable to sending a postcard. By law, employers may monitor telephone calls and e-mail at work.

- Tell a telemarketing company that calls you, "Under the federal Telephone Consumer Protection Act, I want to be on your `do-not-call' list." Sue the company in small-claims court if it does not comply.

- Learn all you can about new technologies. Caller ID, bar codes, skin implants, automated toll systems, video cameras, the Internet, biometrics, genetic tests, airport scanning - all of them affect your rights. Know how they work - what they can do and can't do.

- Ask to inspect your own medical records and add comments to them if they are inaccurate.

- Use two trash cans, splitting in half any documents with vital personal information on them, including Social Security numbers, bank account information, or credit-card numbers. Empty each trash can on alternate weeks.

- Use two phone numbers at home, each with a DISTINCTIVE RING. One is your "public number," which you list on credit applications and in consumer transactions (and give to people you are not crazy about hearing from). When it rings (with its distinctive sound), you will know it is your public line and can decide whether to answer. The other number is your "private number," for close friends and family. Do the same with two addresses. Do the same with two Internet Service Providers and/or electronic-mail accounts.

- Cautiously protect the identities and addresses of your children. Avoid having them enumerated. Keep them off mailing lists by using an adult's name on magazine lists and the like. Don't provide their names on any applications that parents submit.

- If you use the World Wide Web at work or on a computer shared with others, disable "cookies" in your Internet browsing software or delete sensitive "cookies" in the browser. Have a second credit card for use only when you purchase on-line, so that you can conveniently cancel it promptly if it is abused. Try to keep tight control over the use of your photograph on the Web.

- Remember that a government directive requires airlines to ASK for photo ID but also says that airlines should find alternative security measures for passengers who decline. The government does NOT say that you can't fly if you do not display an identity document. The demand for next-of-kin information on international flights is VOLUNTARY.

A MODEL PRIVACY POLICY BY THE PRIVACY JOURNAL

- Organizations establishing privacy policies should incorporate the elements of the widely accepted Code of Fair Information Practice.

- The existence of all data systems with personal information in them should be publicly disclosed, and the purpose for which information is gathered about people should be disclosed. This is the principle of openness or transparency.

- There must be a way for an individual to find out what information about him or her is in a record and how it is used.

- There must be a way for an individual to prevent information about him or her that was obtained for one purpose (which was stated when the information was gathered) from being used or made available, either within the organization or outside, for a purpose that is incompatible with the original purpose, without getting the consent of the individual. This is the principle of secondary use.

- There must be a way for an individual to correct or amend a record that contains information that is identifiable to him or her.

- The organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability, accuracy, security and timeliness of the data. In other words, the custodian of information that is disseminated has an obligation to the individual to make sure it is accurate, secure, and not misused. This obligation ought not be delegated to another entity.

- An organization must make sure that other entities handling personal information in behalf of the first organization are bound by these same principles.

- An organization must conduct periodic risk assessments, balancing the possibility or probability of unauthorized access or disclosure against the cost of security precautions and the expected effectiveness of the precautions. In some cases, it will be necessary to establish an audit trail so that records are kept of disclosures of personal information, both within the organization and outside.

- Organizations must take special precautions in collecting and using personal information about children, both those 13 or younger and those 18 or younger.

- An organization should openly disclose its policies and practices with regard to electronic surveillance of its employees' and customers' telephone calls, electronic mail, Internet usage, changing rooms, and rest rooms. It must articulate in advance the reasons for the surveillance.

- An organization should designate an individual or office (whether full-time or part-time) to handle privacy issues by (a) acting as an ombudsman for customers or employees, (b) assessing the privacy impact of new undertakings, (c) assuring that the organization complies with all laws and trade-association standards; and (d) informing the organization of the latest technology and policies that affect the privacy of customers or employees. An organization, if it utilizes "opt-out" for customers to stay out of certain uses of their information, should make exercising "opt-out" easy, as easy as clicking a button or checking a box, without the need to write a letter or to communicate with another office.

- An organization should conduct periodic training of its employees (and volunteers) to assure that they know (1) applicable laws on confidentiality that govern the organization, (2) the organization's policies and actual practices, (3) the rationale for protecting confidentiality and the sensitivity of personal information, (4) the ability to recognize possible breaches and to report them to the proper person. An organization may chose to certify that employees who handle personal information are properly trained.

ENDNOTES

[1] Schwarz, Reidenberg. Data Privacy Law. 1996.

[2] Schwarz, Reidenberg. Data Privacy Law. 1996.

[3] Givens, Beth. The Privacy Rights Handbook. 1997.

[4] Bonavia, Marjorie, Professor, Ithaca College. *Testimony presented at the New York State Legislative Office Building, Assembly Public Hearing on Personal Privacy*, May 12, 1998.

[5] Bonavia, Marjorie, Professor, Ithaca College. *Testimony presented at the New York State Legislative Office Building, Assembly Public Hearing on Personal Privacy*, May 12, 1998.

[6] PC World Magazine, September, 1998.

[7] Moynihan, Michael. *The Searchable Soul*. Harper's magazine. January 2000.

[8] Swire, Peter. U.S. Chief Counsel for privacy, Office of Management and Budget. *Testimony before the United States Department of Commerce and the Federal Trade Commission, Public Workshop on Online Profiling*. November 8, 1999.

[9] *Direct*. June, 1996.

[10] Southern Maryland Online. 1999.

[11] *CBS NEWS, 1998.*

[12] Lukenbill, Grant. *Consumers Most Worried About Privacy, Polls Find*. DM News. December 29, 1999.

[13] MaryAlice O'Brien, State Legislative Chair, American Association of Retired Persons. *Testimony Before the New York State Senate Majority Task Force on the Invasion of Privacy*. Albany, New York. April 15, 1999.

[14] United States General Accounting Office. *Social Security, Government and Commercial Use of the Social Security Number is Widespread.* February 1999.

[15] Beth Givens. *Identity Theft: How it Happens, Its Impact on Victims, and Legislative Solutions*. Privacy Rights Clearinghouse. August 29, 1999.

[16] Federal Trade Commission. *ID Theft: When Bad Things Happen To Your Good name*. February 2000.

[17] Platt, Suzy (editor). *Respectfully Quoted*: *A Dictionary of Quotations Requested from the Congressional Research Service.* 1989.

[18] *The End of Privacy.* The Economist. May 1, 1999.

[19] Thornburg, Ryan. *Focus on Geographic Information: GIS and the Privacy Puzz*le. Governing. December, 1999.

[20] Powelson, Richard. *Prisoners Cited in Credit Fraud: Report Points to Government Contracts.* Chicago Sun-Times. November 25, 1999.

[21] Powelson, Richard. *Prisoners Cited in Credit Fraud: Report Points to Government Contracts.* Chicago Sun-Times. November 25, 1999.

[22] PC World Magazine, September, 1998

[23] Schwarz, Reidenberg. Data Privacy Law. 1996.

[24] Privacy Rights clearinghouse. *Privacy in Cyberspace: Rules of the Road for the Information Superhighway*. 1999.

[25] Hansell, Saul. *You've Got Mail, Films, Tunes*… Albany Times Union. January 11, 2000.

[26] *The End of Privacy.* The Economist. May 1, 1999.

[27] Clausing, Jeri. *Report Rings Alarm Bells About Privacy on the Internet*. New York Times. February 7, 2000.

[28] PC World Magazine, September, 1998

[29] Meyer, Howard. *Technology and the Loss of Information Privacy*. Computers & Law. Fall 1996.

[30] Privacy Rights clearinghouse. *Privacy in Cyberspace: Rules of the Road for the Information Superhighway*. 1999.

[31] Schwarz, Reidenberg. Data Privacy Law. 1996.

[32] Schwarz, Reidenberg. Data Privacy Law. 1996.

[33] Schwarz, Reidenberg. Data Privacy Law. 1996.

[34] United States General Accounting Office. *Social Security, Government and Commercial Use of the Social Security Number is Widespread.* February 1999.

[35] Segal, David. *FTC Blocks Credit Firm's Selling of Personal Data*. The Seattle Times. August 27, 1998.

[36] Segal, David. *FTC Blocks Credit Firm's Selling of Personal Data*. The Seattle Times. August 27, 1998.

[37] Brooks, Rick. *Equifax to Buy Division of Polk For $260 Million*. Wall Street Journal. February 10, 2000.

[38] The Center for Media Education's report Web of Deception: *Threats to Children from Online Marketing. 1999.*

[39] Federal Trade Commission. *How to Comply With The Children's Online Privacy Protection Rule*. November, 1999.

[40] Federal Trade Commission. *How to Comply With The Children's Online Privacy Protection Rule*. November, 1999.

[41] Federal Trade Commission. *How to Comply With The Children's Online Privacy Protection Rule*. November, 1999.

[42] Federal Trade Commission. *How to Comply With The Children's Online Privacy Protection Rule*. November, 1999.

[43] Sykes, Charles. *The End of Privacy*. 1999.

[44] Privacy Rights Organization. *How Private is my Medical Information*. 1999.

[45] PC World Magazine, September, 1998.

[46] PC World Magazine, September, 1998.

[47] *Court Sustains Patients' Suit Over Pharmacy's Use of Prescription Data*. Pharmaceutical Litigation Reporter. August 1999.

[48] Privacy Rights Organization. *How Private is my Medical Information*. 1999.